

A study regarding the effectiveness of game play as part of an information security awareness program for novices

by

**WILLIAM AUBREY LABUSCHAGNE**

submitted in accordance with the requirements

for the degree of

**MAGISTER TECHNOLOGIAE**

in the subject

**INFORMATION TECHNOLOGY**

at the

**UNIVERSITY OF SOUTH AFRICA**

SUPERVISOR: PROF MM ELOFF

CO-SUPERVISOR: DR L LEENEN

SEPTEMBER, 2015

## DECLARATION

I declare that "A study regarding the effectiveness of game play as part of an information security awareness program for novices" is my own work and that all sources that I have used or quoted have been indicated and acknowledged by means of complete references.



-----  
William Aubrey Labuschagne  
(Student Number: 4729-802-2)

16-09-2015

-----  
Date

## Acknowledgements

I wish to express my sincere appreciation to:

- Prof Eloff, teaching me everything I now about the process of completing a dissertation and becoming a better researcher in the field of information security. Your assistance, patience and kind words of advice to see if there is a better way to do things have been inspirational. You have created a warm space filled with trust which encourages exploration of ideas. Thanks for creating an environment to allow me to be me.
- My wife, Namosha, who has stood by my side from the start to the end. I am grateful for your compassion, understanding and providing a helping hand in my pursuit of this milestone in our lives. We have had many challenges in this pursuit but together we have conquered them and grown stronger. Happiness means nothing unless shared; this journey was worth sharing with you.
- My parents who believed in me to follow my dreams and use the opportunities given to make a difference. You have instilled a strong value system to believe in myself, never give up and live life to the fullest. This dissertation is part of my journey that you have helped to create for me. My upbringing by you has had a great impact on me to complete this journey of self discovery and making a difference in society.
- To my family members, thank you for all the encouragement, advice and moral support. To the family members who have started the journey with me but are no longer here, I miss you and I wish you could be here to share this moment. I was blessed with your support throughout the challenging times, it will never be forgotten.
- Friends and work colleagues whom aided me emotionally and technically during this exploration of information security awareness. There are too many names to mention however Joey Jansen van Vuuren who created the opportunity and provided access to support structures needs to be highlighted. There were times were I started doubting the cause pursued. The backing from the collective helped me to see the light in times of darkness.
- Dr Zaaiman and the University of Venda, for providing an opportunity to conduct an information security awareness program within their organization. All the individuals

that were involved during the execution of the awareness program were selfless and were a joy to work with.

- The Council for Scientific and Industrial Research (CSIR), especially CyberDefence (within Defence, Peace, Safety and Security (DPSS)), for providing an environment to pursue research in the domain of information security. In addition, providing support structures to assist in the process to complete the dissertation and create opportunities to network with other institutions and individuals on the subject matter.
- All people who have supported me emotionally and technically during this journey to learn about information security awareness and subsequently to give back to society.



## **Abstract**

Technology has become intertwined into society daily life which is not only limited to personal life but also extending into the business world. Availability, integrity and confidentiality are critical information security factors to consider when interacting with technology. Conversely many unsuspecting users have fallen prey to cyber criminals. The majority of threats encountered could have been prevented by the victims if they had sufficient knowledge to first identify and then mitigate the threat. The use of information security awareness programs provides a platform whereby users are informed about such threats. The success of these programs is significantly reduced if the content is not transferred in the most effective method to improve understanding and result in a change of behaviour.

This dissertation addresses the effectiveness of using a gaming platform within an information security awareness program. The use of games allows for the users to apply knowledge within a potential scenario as seen with pilots using flight simulators. End users who have no information security background should have a safe platform where threats can be identified and methods taught to mitigate the threats. A wide selection of security awareness frameworks exist, the most appropriate framework should be considered first. The different phases of the framework would be applied within the dissertation with the main objective to ultimately determine the effectiveness of games within security awareness programs.

Data was collected during the implemented information security awareness program using quantitative instruments. These included questionnaires and a developed online game designed from the literature reviewed during the study. The analysed data highlighted the effects of extrinsic motivation on knowledge transfer and validated the positive impact of game play.

## Table of Contents

<b>Acknowledgements</b>	<b>ii</b>
<b>Abstract</b>	<b>iv</b>
<b>List of Figures</b>	<b>viii</b>
<b>List of Tables</b>	<b>x</b>
<b>List of Abbreviations</b>	<b>xi</b>
<b>Chapter 1: Introduction and Research Objectives</b>	<b>1</b>
1.1 The Case for Information Security Awareness	1
1.2 Motivation for this Study	2
1.2.1 End users' susceptibility to cyberthreats originating from the Internet:	2
1.2.2 Identifying relevant topics for a specific information security awareness target group:	3
1.2.3 Deploying effective information security awareness programs:	4
1.2.4 Conclusion	5
1.3 Problem Statement	5
1.3.1 Determine what is the current information security knowledge of information security novices?	5
1.3.2 What threat categories should be included in an information security awareness program for information security novices?	6
1.3.3 How effective are lecture based information security awareness programs?	7
1.3.4 How is the effectiveness of an information security awareness program measured?	7
1.3.5 What components are found in an information security awareness program?	7
1.3.6 How effective are games as a platform to deliver information security awareness?	8
1.3.7 Conclusion	8
1.4 Scope and Purpose (Research Objectives)	8
1.5 Research Methodology and Process	9
1.6 Terminology	12
1.7 Dissertation Layout	13
<b>Chapter 2: Information Security Awareness</b>	<b>15</b>
2.1 Introduction	16
2.2 What is Information Security?	16
2.3 Importance of Information Security	17
2.4 Security Controls used within Information Technology	23
2.4.1 Effectiveness of updates to operating systems	23
2.4.2 Effectiveness of anti-virus software	25
2.4.3 Effectiveness of firewalls	26
2.4.4 Conclusion	27
2.5 Information Security Awareness	29
2.5.1 Definition	29
2.5.2 Case Study	29
2.5.3 Outcomes	30
2.5.4 Point of Failure	31
2.6 Conclusion	33
<b>Chapter 3: Information Security Awareness Program</b>	<b>35</b>
3.1 Introduction	36
3.2 Standards addressing Information Security Awareness	37
3.3 Information Security Awareness Frameworks	38
3.4 European Network and Information Security Agency (ENISA)	39
3.4.1 Overview	39
3.4.2 Plan, Assess and Design	42
3.4.3 Execute and Manage	45
3.4.4 Evaluate	46
3.4.5 Evaluation Result of ENISA Information Security Awareness Framework	46
3.5 SANS Information Security Awareness Roadmap	47
3.5.1 Overview	47

3.5.2	Evaluation Result of SANS Information Security Awareness Framework	51
3.6	National Institute of Standards and Technology (NIST) Security Framework	52
3.6.1	Overview	52
3.6.2	Evaluation Result of NIST Information Security Awareness Framework	55
3.7	Selection of Information Security Awareness Framework	56
3.8	Conclusion	57
<b>Chapter 4: Using NIST within an Information Security Awareness Program</b>		<b>59</b>
4.1	Introduction	60
4.2	NIST Security Framework	60
4.2.1	Design	61
4.2.2	Development	62
4.2.3	Implementation	62
4.2.4	Post Implementation	62
4.3	Conclusion	63
<b>Chapter 5: Design of Information Security Awareness Program</b>		<b>65</b>
5.1	Introduction	66
5.2	Needs Assessment from Shared Resources	66
5.2.1	The Internet Café Industry in South Africa	67
5.2.2	Internet Uses and Threats Mapping	68
5.2.3	Selection of Topics	70
5.3	Needs Assessment from Social Networking Sites	74
5.3.1	Related Research	74
5.3.2	Social Media Profiling Experiment	77
5.3.3	Application of Data Collected to Conduct a Social Engineering Attack	85
5.4	Topics Identified for an Information Security Awareness Program	86
5.5	Conclusion	89
<b>Chapter 6: Development (Distribution Platform)</b>		<b>93</b>
6.1	Introduction	94
6.2	Shared Public Security Awareness (SPSA) System	95
6.2.1	Requirements	96
6.2.2	Shared Public Security Awareness (SPSA) System Architecture	101
6.2.3	Conclusion	109
6.3	Design Consideration of an Information Security Awareness Program through Gaming	110
6.3.1	Gaming Motivation	110
6.3.2	Requirements	114
6.3.3	Conceptual Game Prototype	118
6.4	Conclusion	123
<b>Chapter 7: Implementation (Data Collection)</b>		<b>125</b>
7.1	Introduction	126
7.2	Research Design	126
7.2.1	Interviews	130
7.2.2	Surveys and Questionnaires	131
7.3	Methodology	134
7.3.1	Research Instruments	134
7.3.2	Game Events	143
7.3.3	Data	144
7.4	Limitations	147
7.5	Ethical Consideration	148
7.6	Conclusion	151
<b>Chapter 8: Post Implementation (Analysis of Data)</b>		<b>153</b>
8.1	Introduction	154
8.2	Analysis	154
8.2.1	Analysis of the questionnaire data	154
8.2.2	Analysis of the online gaming data	161
8.3	Findings	174
8.4	Conclusion	175

<b>Chapter 9: Conclusion</b>	<b>177</b>
9.1 Introduction	178
9.2 Revisiting the Problem Statement	178
9.3 Main Contribution	183
9.4 Future Work	184
9.5 Publications	185
<b>10 References</b>	<b>186</b>
<b>Appendix A Ethical Clearance Certificate</b>	<b>198</b>
<b>Appendix B Questionnaire (Pre Assessment)</b>	<b>199</b>
<b>Appendix C Questionnaire (Post Assessment 1)</b>	<b>209</b>
<b>Appendix D Questionnaire (Post Assessment 2)</b>	<b>220</b>
<b>Appendix E Unique Identifier List</b>	<b>231</b>
<b>Appendix F Consent Form</b>	<b>233</b>
<b>Appendix G Published Papers</b>	<b>234</b>

## List of Figures

Figure 1-1: Layout of Dissertation	14
Figure 2-1: Layout of Chapter 2	15
Figure 2-2: Information Technology Security Techniques	23
Figure 2-3: Information Technology Security Controls	28
Figure 2-4: Point of Failure Model	32
Figure 3-1: Layout of Chapter 3	35
Figure 3-2: Relationship between Standards, Frameworks and Security Programs	36
Figure 3-3: ENISA Information Security Awareness Processes	40
Figure 3-4: European Network and Information Security Agency Framework	41
Figure 3-5: Basic Communication Components	44
Figure 3-6: SANS Information Security Awareness Roadmap	48
Figure 3-7: NIST Framework	52
Figure 3-8: Revised Awareness and Training Program Plan (NIST)	55
Figure 4-1: Layout of Chapter 4	59
Figure 4-2: Mapping of NIST Phases to Dissertation Chapters	60
Figure 5-1: Layout of Chapter 5	65
Figure 5-2: Needs Assessment	66
Figure 5-3: Threat Vectors for Internet Café	73
Figure 5-4: Data Disclosure	81
Figure 5-5: Results from Friendship Requests	82
Figure 5-6: Negative Emotions from Posts Analysis	83
Figure 5-7: Anger Emotions above 10%	84
Figure 5-8: End User Attack Tree	89
Figure 6-1: Layout of Chapter 6	93
Figure 6-2: Capabilities of Shared Public Security Awareness System	97
Figure 6-3: EasyHotspot Management System	99
Figure 6-4: Internet Access System	102
Figure 6-5: Daily Virtual Machine Operations	103
Figure 6-6: URL Inspector	105
Figure 6-7: Awareness Collection System	107
Figure 6-8: Awareness Content System	109
Figure 6-9: CyberProtect Interface	113
Figure 6-10: Game Design Requirement	114
Figure 6-11: TAM Model	117
Figure 6-12: Extended TAM Model	118
Figure 6-13: High-level Design of Game	119
Figure 6-14: High Level View of Game Prototype	120

A study regarding the effectiveness of game play as part of an  
information security awareness program for novices

---

Figure 6-15: Mixture of Hypertext and Hypermedia	121
Figure 6-16: Sample Question and Status	122
Figure 6-17: Badges and Achievements	123
Figure 7-1: Layout of Chapter 7	125
Figure 7-2: Time-Series Research Design with an Intervention Group and a Control Group	127
Figure 7-3: Content and Processes of an Information Security Workshop	128
Figure 7-4: Data Collection Process	135
Figure 7-5: Spacing Effect (De la Rouviere 2012)	136
Figure 7-6: Example of Online Questionnaire Questions	139
Figure 7-7: Achievement Badges	141
Figure 7-8: Inventory Items	142
Figure 7-9: CyberAwareness Social Networking Site Game	143
Figure 8-1: Layout of Chapter 8	153
Figure 8-2: Questionnaire Results (Average)	155
Figure 8-3: Assessment Box Plots	156
Figure 8-4: Distribution of Assessment Marks	157
Figure 8-5: Line Graph Comparing Results (Mean and TrimMean)	159
Figure 8-6: Line Graph Comparing Results (Mean and Median)	159
Figure 8-7: Formula for STDEVP	160
Figure 8-8: Line Graph Population Standard Deviation	160
Figure 8-9: Formula for VARP	161
Figure 8-10: Line Graph Population Standard Deviation	161
Figure 8-11: Total Responses (5 Minute Intervals)	163
Figure 8-12: Response Classification (Correct and Incorrect Responses)	164
Figure 8-13: Correct and Incorrect Responses	164
Figure 8-14: Average Response Time	166
Figure 8-15: Distribution of Awareness Topics	168
Figure 8-16: Line Graph of Correct and Incorrect Responses for each Topic	169
Figure 8-17: Average Scores for Topics (Questionnaires)	170
Figure 8-18: Comparison of average scores per Questionnaire for each Topic	171
Figure 8-19: Comparing Post Assessment 1, Online Game and Post Assessment 2 Results	172
Figure 9-1: Layout of Chapter 9	177

## List of Tables

Table 1-1: Terminology	12
Table 3-1: SANS Supporting Documents	49
Table 3-2: Example of Information Security Awareness Metric Table	51
Table 3-3: Selection Criteria for Frameworks	56
Table 5-1: Classification of Internet Uses	69
Table 5-2: Mapping of Internet Uses to Threats	71
Table 5-3: Status description	79
Table 7-1: List of Information Security Awareness Data Collection Used	130
Table 7-2: Example of List with Unique Numbers	133
Table 7-3: Survey Schedule	138
Table 7-4: Information Security Awareness Topics	138
Table 7-5: Game Events	144
Table 8-1: Online Gaming Topic Response Distribution	167
Table 8-2: Topic Breakdown for each Questionnaire	170

## List of Abbreviations

API	Application Programming Interface
ARC	Archival File Format
BIOS	Basic Input Output System
CMS	Content Management System
CSIR	Council for Scientific and Industrial Research
DHS	Department of Homeland Security
DLL	Dynamic Link Library
DOS	Denial of Service
E - AM	E - Awareness Model
ENISA	European Network and Information Security Agency
EU	European Union
FISMA	Federal Information Security Management Act
GLBA	Gramm-Leach-Bliley Act
HCI	Human Computer Interface
HIMIS	Human Impact Management for Information Security
HIPAA	Health Insurance Portability and Accountability Act
IDS	Intrusion Detection Systems
IE	Internet Explorer
IEC	International Electro Technical Commission
IPS	Intrusion Prevention System
ISO	International Standards Organisation
ISP	Internet Service Provider



A study regarding the effectiveness of game play as part of an  
information security awareness program for novices

---

IT	Information Technology
IVT	Interactive video training
JS	JavaScript
LIWC	Linguistic Inquiry and Word Count
MC	Missouri – Columbia
MCC	Malware Collection and Classification
MIRA	Movement for Islamic Reform in Arabia
MU	University of Missouri Columbia
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PDF	Portable Document Format
PE	Perceived Ease of Use
PHP	Personal Hypertext Preprocessor
POODLE	Padding Oracle On Downgraded Legacy Encryption
PP	Perceived Playfulness
PS	Perceived Security
PU	Perceived Usefulness
SANS	SysAdmin, Audit, Networking, and Security
SE	Social Engineering
SNS	Social Networking Sites
SOX	Sarbanes-Oxley Act

A study regarding the effectiveness of game play as part of an  
information security awareness program for novices

---

SPSA	Shared Public Security Awareness
SWF	Shockwave Flash
TAIS	Teachers Awareness of Internet Safety
TAM	Technology Acceptance Model
TUT	Tshwane University of Technology
UAE	United Arab Emirates
UNISA	University of South Africa
UNIVEN	University of Venda
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
VARP	Variation on the Population
VM	Virtual Machine

## **Chapter 1: Introduction and Research Objectives**

### **1.1 The Case for Information Security Awareness**

The Internet has become an integral part of society. It has no boundaries, and the capabilities provided in the form of services and products allow society to function more efficiently. These services include, but are not limited to, access to education, business functions, searches for information, and social networking. Social networking sites have increased in popularity and are utilised for many purposes, which include connecting with other people, sharing information and creating content (Subrahmanyam, Reich, Waechter & Espinoza 2008). The main objective of the Internet is to add value to society by providing a collaborative platform to connect users from different corners of the world (Papacharissi & Rubin 2000). However, duality exists in all parts of society, as in the case of pharmaceuticals originally developed drugs to cure illness but which can also cause addiction or death with overuse. Another example of duality is seen with automated teller machine where the main purpose was improving accessibility to money but criminals are also targeting these devices.

Cybercrime is a lucrative endeavour for criminals. It can be defined as using the Internet or computer technology to conduct criminal activities (Dictionary.com 2012a). Cybercriminals have a wide variety of tools and techniques available to target unsuspecting computer users, including phishing, spam, denial of service attacks, click fraud, invasion of privacy and defamation, to name but a few (Kim, Jeong, Kim & So 2011). Another tool is malicious software also known as malware, which poses a significant security threat as the attacker can gain control over a computer system (Sophos 2013).

Malware can only be user-activated, which means the user's action is the determining factor in the infection process. The behaviour of the user depends on the intention of the action and the user's expertise level, based on tacit knowledge on how to behave in a certain situation. Dodge (2007); Eminağaoğlu, Uçar and Eren (2009); and Rezgui and Marks (2008) reported a positive change in end-user behaviour after exposing users to computer and information security awareness programs. Involving the users in information security awareness programs does improve awareness and also helps users to retain the acquired knowledge (Albrechtsen & Hovden 2010). Cone, Irvine, Thompson and Nguyen

(2007) reported the effectiveness of information security awareness programs can be improved by the choice of delivery method used to transfer the knowledge.

Information security awareness programs usually consist of different steps namely: design, development, implementation and post implementation. Internet users require effective information security awareness programs to curb the spreading of exploitation, which further strengthens the cybercriminal economy. Society's usage of services within cyberspace provides cybercriminals with additional incentives to ensure the development of strategies to target unsuspected users through the Internet (Sood, Bansal & Enbody 2013). They described how data generated by users interacting with services within cyberspace could be used within the underground economy of cybercrime. For example, a user's computer system could be infected with a malware resulting in the loss of critical information which includes but is not limited to credit card details and authentication data. The harvested data could in turn then be sold within the cybercrime markets (Allodi, Corradin & Massacci 2015).

This study was motivated by the importance of protecting users from threats originating from the Internet through effective information security awareness programs. The term "novice" would refer to a group of end users who does not have an information security background which include employees and home users.

## **1.2 Motivation for this Study**

In the field of information security awareness, numerous problems have been identified. These include but are not limited to:

### **1.2.1 End users' susceptibility to cyberthreats originating from the Internet:**

Many threats originating from the Internet are sophisticated, luring unsuspecting users into performing actions which ultimately infect their systems with malicious software. For example, the multi-platform computer worm Koobface compromised between 400,000 and 800,000 computers during its peak in 2010 (Protalinski 2012). It leveraged social networking sites to propagate and infect computer systems. Provocative messages were sent to Facebook users to direct them to videos of a sexual nature. Once they clicked on the link within the message, these users were instructed to download a video codec to view the content. As a result of downloading and installing the 'video codec', users'

systems became infected with malware (Thomas & Nicol 2010). This exploitation could have been mitigated if the users had been aware of this malicious attack technique.

Another example is the threat of cybercriminals using well-known personalities to entice users to willingly divulge personal information. Criminals created a Facebook page called “*R.I.P. Steve Jobs*” after his passing on 5 October 2011. The page contained a malicious Uniform Resource Locator (URL) and manipulative text claiming that 50 free iPads were available. This URL led to a page where users had to provide personal information, including their name, email address, telephone number and physical address (Panda Security 2011). The attackers used this event to lure unsuspected users into a scam. These users would have been better equipped to recognise this scam if they had attended an information security awareness program that focused on scams. The mitigation of this threat forms part of information security awareness training. Moreover, Rossman (2010) reported on the cost of Internet-based scams and fraud in the United States of America (USA) which doubled from 2008 to \$559.7 million in 2009. The cost of online fraud was estimated to be exceeding \$100bn in 2013 (McDonald 2013). Again, information security awareness could have prevented victims falling prey to these threats. Therefore, a lack of information security awareness amongst Internet users has been identified.

### **1.2.2 Identifying relevant topics for a specific information security awareness target group:**

The ultimate objective of information security awareness programs is to harden users, make them more resistant to attacks. It should be noted that information security awareness programs does not prevent end-user to be targeted and subsequently attacked. Effectiveness can be measured by observing a behavioural change of computer users after an information security awareness program. It is important to understand what obstacles could be encountered that could impede on the success of the information security awareness program. Russell (2002) listed the use of a “one-size-fits-all” strategy as an ineffective implementation of information security awareness; this is as an approach that does not customise the content to fit the needs of a specific information security awareness training audience. In other words, the content should be relevant to the people attending the training. For example, Kruger and Kearney (2005) implemented an information security awareness program at the international mining company AngloGold Ashanti in Ghana. The program was designed to address the company’s specific needs, including the adherence to company policies, use of mobile equipment, email use,

reporting on incidents and password usage customised for the employees in Ghana. The content of the above mentioned information security awareness program implemented by Kruger and Kearney does not address the needs of a user who only accesses the Internet at home. Such a user is exposed to additional threats, for example fake online personas located on social networking sites, cyberbullying and privacy. The AngloGold Ashanti company's policy is not applicable to every home user, therefore awareness topics related to AngloGold Ashanti will also not be sufficient for home users.

The topics addressed by the information security awareness program are essential to the success of these programs.

### **1.2.3 Deploying effective information security awareness programs:**

Information security awareness programs are designed and developed to change the behaviour of computer users in order to mitigate threats encountered while using computer systems, including accessing the Internet. Due to the broad use of computer systems, some threats can only be mitigated by service providers. A Denial of Service (DoS) attack, for example, originates outside of the computer system. This type of attack is considered to be technically complex for the average home user to mitigate. The user could apply all operating system patches and not perform any action and still be attacked by a DoS attack. A DoS attack can only be mitigated by the Internet Service Provider (ISP).

However, information security awareness programs should prescribe effective behavioural changes, for example, not opening an email with a file attachment from an untrusted or unknown source. Consider the research of Dodge (2007), who evaluated users' responses to phishing attacks via emails. A system was developed to create phishing attacks within a controlled environment to determine if the information security awareness program was effective. The information security awareness program focused on phishing attacks. One of their goals was a decline in users who fall prey to phishing attacks. The results demonstrated that exposure to the information security awareness content over time resulted in fewer users being lured into phishing attacks. This specific awareness program proved to be an effective strategy to empower users with phishing attack mitigation techniques. Consequently, the research undertaken for this study required the development and deployment of a system which could measure the effectiveness of an implemented information security awareness program.

#### **1.2.4 Conclusion**

Several problems were identified within the domain of information security awareness on the basis of numerous reports, case studies and academic papers highlighting the weakness of the human factor. The following section lists research questions addressing essential components required for an effective information security awareness program.

### **1.3 Problem Statement**

The use of technology has become ubiquitous resulting in the upsurge of cybercriminal activities conducted by cybercriminals who have seized the opportunity to profit from unsuspecting end users (Sood et al. 2013). Security controls used to protect the end user have become less effective in recent times. The end user has been identified as the weakest link in the information security chain. Attacks originating from cybercriminals can be prevented with the use of information security awareness programs. The effectiveness of information security awareness programs are subject to design and development factors and the identification of success factors are critical to ensure knowledge transfer occurs.

The following subsections list fundamental questions required for the implementation of an information security awareness program that effectively changes the end user's behaviour.

#### **1.3.1 Determine what is the current information security knowledge of information security novices?**

The measurement of the information security knowledge of information security novices is a critical step in identifying a need, if any, for information security awareness training. Once a need has been identified, measures could be applied to address the need.

The term "information security novices" refers to computer users who do not have an information technology background or have not received information security awareness training. These users can also be called "home users", if not employed in organisations where computers are used on a daily basis. Usually they have inadequate knowledge to understand the underlying computer system architecture and potential effects of system configuration. Such a user is usually not capable of performing the following preventative actions: modifying the web browser to protect privacy, configuring the operating system to improve security, disabling services to improve computer system performance and most importantly understanding the different security threat vectors which could target them.

The use of computers and the Internet have become an integral part of everyday life and the dependence on these platforms requires users to protect themselves against attacks from cybercriminals. Users can only act responsibly once they become aware of the threats which they can encounter and if they have been provided with appropriate mitigation techniques to protect themselves and their computer systems. Numerous reports indicate this is not happening, as cybercrime as well as malware is on the rise. Barlowe and Blackbird (2012) reported on the increase of malware and threats from about 1000 types of malware in 1991 to 60000 types of malware in 2001. RSA (2012), a well-known security company, reported that about 232 computers are infected with malware every 60 seconds. In 2015, the estimated total number of malware listed exceeded 350 million samples (AV-TEST 2015). A security threat report by Sophos (2014) highlighted an expansion of the threat vectors, which now include mobile devices, as well as an increase in the complexity of malware targeting operating systems, even Linux and Mac operating system (OS) X.

### **1.3.2 What threat categories should be included in an information security awareness program for information security novices?**

Topics covered in information security awareness training material should be relevant to the users who are attending the training. Consider the case of information security novices who do not have technical knowledge about the information technology (IT) field. These users use computers ubiquitously as part of everyday living, e.g. shopping online, checking email, looking for information, playing and downloading music, watching movies, and keeping in contact with friends on social networking sites. However, the majority of these users do not understand the concept of a DoS attack, a rootkit, polymorphic malware, virtualisation or the differences between web browsers. A knowledgeable IT user would understand these terms and know how to configure a computer for optimal use while still providing a secure useable system.

Information security awareness training should address mitigation techniques which are relevant to threats the end user may encounter, e.g., selecting a strong password. The identification of the threat categories, which could be used to target information security novices, has a two-fold advantage. Firstly, these categories can be used as part of the information security awareness development process; secondly, the content will be more relevant to specific types of users.



### **1.3.3 How effective are lecture based information security awareness programs?**

The content and the delivery of an awareness program are important. Previous work from Cone et al. (2007); Albrechtsen and Hoven (2010); and Rhee, Kim and Ryu (2009) have shown that the understanding and retention of knowledge are determined by the method with which the programs are presented to the users. An understanding of what an awareness program should consist of is needed. Wilson and Hash (2003) provided some guidelines on the topic of developing an awareness program. Khan, Alghathbar, Nabi and Khan (2011) described many methods of delivery, including posters, lecture-based training, web-based training, email and presentations. It is critical to understand which method is the most effective to ensure that resources are not wasted and that the learning process is optimized. Training conducted in the form of lectures is widely used and the effectiveness of this method needs to be determined.

### **1.3.4 How is the effectiveness of an information security awareness program measured?**

The main objective of an information security awareness program is to transfer computer security-related knowledge to users who have been identified with a lack in the necessary skills to protect themselves and their computer system from threats originating from cyberspace. The success of an information security awareness program is determined by the effective application of the acquired knowledge. An understanding of the different techniques used for transferring information security awareness is required to understand how to measure the effectiveness of these knowledge transfer sessions and to improve current information security awareness programs to the best benefit of the users who participate. The transfer of knowledge occurs during training sessions which forms part of an information security awareness program.

### **1.3.5 What components are found in an information security awareness program?**

An information security awareness program consists of different steps to be executed in a sequence to ensure successful deployment and implementation. Each step has outputs, which are used as input to the next step. Several information security awareness programs exist but only the European Network and Information Security Agency (ENISA); the SysAdmin, Audit, Networking and Security (SANS); and the National Institute of Standards and Technology (NIST) will be considered for this study. The components within a security

awareness program must be identified and fully understood to effectively implement the program.

### **1.3.6 How effective are games as a platform to deliver information security awareness?**

Games have been widely adopted not only for entertainment, but also for educational purposes. An example of a social networking game is Farmville which provides entertainment while teaching the user about farming concepts (Liszkiewicz 2010). Games have become an effective mechanism to transfer knowledge to the user in a natural manner. For example, flight simulator games provide users with a realistic feeling and the skills to fly an aircraft without climbing into the cockpit of an aircraft and endangering themselves and society. Huizenga, Admiraal, Akkerman and Ten Dam (2009) concluded that pupils remembered more information with game play due to the realistic and meaningful presentation of the content. The effectiveness of using games within information security awareness programs needs to be determined as this could form part of an effective information security awareness program.

### **1.3.7 Conclusion**

Several inquisitive questions have been identified in the previous subsections to explore the different components required for an effective information security awareness program. The remaining chapters in this dissertation address each of the questions identified. Answering these questions lead to an understanding of the components required to deploy an effective information security awareness program and focus on the impact of gaming within information security awareness.

## **1.4 Scope and Purpose (Research Objectives)**

The scope of this dissertation covers the use of social networking games to deliver effective information security awareness content targeted at information security novices. Many users who work within corporate companies are protected by security measures enforced by the company which are not always transparent to the user; for example, the use of sophisticated firewalls, implementation of anti-malware software which automatically update, the backup of data and controlled Internet access. These users are automatically protected, and in most cases they are also required to attend information security awareness programs. Many home computer users do not have these privileges and cannot implement these countermeasures at home due to financial constraints and

lack of technical knowledge. Innovative solutions are required to address educating all of society regarding the threats of the cyberworld and to ensure the successful deployment of effective countermeasures to ensure knowledge transfer and retention.

The purpose of this research is to determine the effectiveness of gaming as a component of information security awareness programs. Humans have a tendency to forget knowledge which is not used. The use of games that focus on information security awareness topics could provide a platform to retain the knowledge acquired during an information security awareness program for longer periods. The effective deployment of information security awareness programs forms a critical component of the drive to fight cybercrime.

Industry sectors such as financial systems, transportation, information technology, communications, emergency services and security systems depend on the availability, confidentiality and integrity of information within the cyberworld. These sectors can also be defined as the critical infrastructures which are essential to the functioning of society. An attack on these sectors could detrimentally disrupt the functioning of society and provide a threat to national security.

Users of any computer system must be educated on the threats and be provided with mitigation techniques to prevent exploitation. The education process includes the use of information security awareness programs and the effectiveness of these programs is critical to success.

## **1.5 Research Methodology and Process**

This section discusses the research methodology best suited for this study. The metaphor of the “Research Onion” developed by Saunders, Lewis and Thornhill (2012) is applied in designing a research methodology. The philosophical stance on the effectiveness of gaming as part of an information security awareness program is described first. The reasoning process required to select the best suited research philosophies ensures the author understands the information security awareness. This could assist the author in identifying the type of data, collection methods and the interpretation of the data necessary to answer the problem questions. The identification of the most suited research approach and strategy would be described thereafter.

The objective of the research is determining whether the use of gaming as a delivery platform could be used to enhance the effectiveness of an information security awareness program. Knowledge transfer would be a critical in the gaming component of the information security awareness program. The understanding and recalling of the newly acquired knowledge is governed by fundamental laws of learning by human memory and can be objectively observed however the individuals' perceptions would also affect the knowledge learned. Therefore, the research conducted within this study would take a realism philosophy approach as human subjects would form part of the study also the experience would be allow the participants to adapt their perceptions within a socially constructed environment (Saunders & Tosey 2012).

Several abstract concepts could be formulated on effective knowledge transfer within information security awareness to design and develop a concrete experience by testing the concepts within a new situation. The resulting experience would in turn allow the author to observe relationships between the variables subsequently reflecting on the results. This iterative process would similar to the experiential learning cycle designed by Kolb (1984). Therefore a deductive research approach would be taken during this research.

Different research strategies are available to conduct the research within this study which include but is not limited to experimental research, action research, interview and case study research (UK Essays 2013). Due to the limited variables under investigation during this study as well as the comparison of the end with the expected results the research strategy considered for this study is a combination of experimental research and surveys. Bryman and Bell suggests the latter is commonly used if the sample represents a portion of the population and if the data can be empirically analysed to delve into the relationships between the variables (2011).

The research would be conducted in a short time frame due to limited funding and availability to participants during the study therefore a cross-sectional time horizon would be selected (UK Essays 2013). Data would be collected from primary and secondary data sources. Several sensors would be designed and developed to collect primary data from the participants during the study which include questionnaires and a gaming platform. Secondary data sources would focus on work conducted by other researchers in the

domain of information security awareness and other related domains which include education and management sciences.

In conclusion, this section gave an overview of the research process followed to determine the effectiveness of game playing in information security awareness programs. The next section describes the terminology used within this dissertation.

## 1.6 Terminology

Table 1-1 lists the terminology used in this dissertation.

**Table 1-1: Terminology**

Term	Description
Computer System	All the components (including software and hardware) allowing the computer to work independently and with other remote computers through a networked platform, subsequently performing a desired process (Mano 1993).
Cybercrime	Activities originating from a computer system that are against the law and results in any harm to an end user or other computer system (Britz 2009).
Cyberspace	Networked platforms which are interconnected and allows the dissemination of information and access to shared resources which include the Internet (Kitchin 1998).
Digital Footprint	Data generated by end user activities within cyberspace as seen by other end users and providing personal information of activities on social networking sites (Madden, Fox, Smith & Vitak 2007).
End User	A person who interacts with a computer system to achieve a specific goal (Rockart & Flannery 1983).
Gamification	Use of game elements within a non-game context to promote engagement (Yohannis et al. 2014).
Information Security Awareness	Provides computer end users with the necessary knowledge and skills to identify and mitigate threats targeting the computer system or other entities using the computer system which include the computer user (Thomson & von Solms 1998).
Information Security Novices	Describes a computer user who has not received any formal training on the subject of information security or has attended an information security awareness program. In other words, users who do not have the technical security skills to make informed decisions regarding information security are considered to be novices.
Malicious Payload	Malicious software encapsulated in a delivery mechanism and transported to target (Wikia 2015).
Social Networking Site Game	A gaming component accessed by end users though a social networking platform, with the main objective to play the game and in some cases compete with other end users on the platform (Barnes & Barnes 2009).
Threat Vector	A potential vulnerability which could be exploited by cybercriminals (Chen, Boehm & Sheppard 2007).
Zero Day Vulnerability	A vulnerability that can be used to exploit systems with no prevention mechanism available as is has not been disclosed to the security vendors (Bilge & Dumitras 2012).

## 1.7 Dissertation Layout

The previous sections of this chapter introduced the background to, research methodology of and problem statements addressed by this research. The dissertation consists of several chapters covering the research conducted.

**Chapter 1** introduces the dissertation topic by providing background information on the problems identified within the field of information security awareness.

**Chapter 2** describes the importance of information security awareness programs. The chapter includes a summary of the current worldwide state of cybersecurity and elaborates on the threats posed by cybercriminals.

**Chapter 3** discusses the different information security awareness frameworks considered for this study. Subsequently one framework is selected for use within this study.

**Chapter 4** explains the components required for a successful information security awareness program, which include design, development, implementation and post-implementation of such a program.

**Chapter 5** assesses the need for information security awareness and identifies the topics required for information security novices who frequently access the Internet using shared resources.

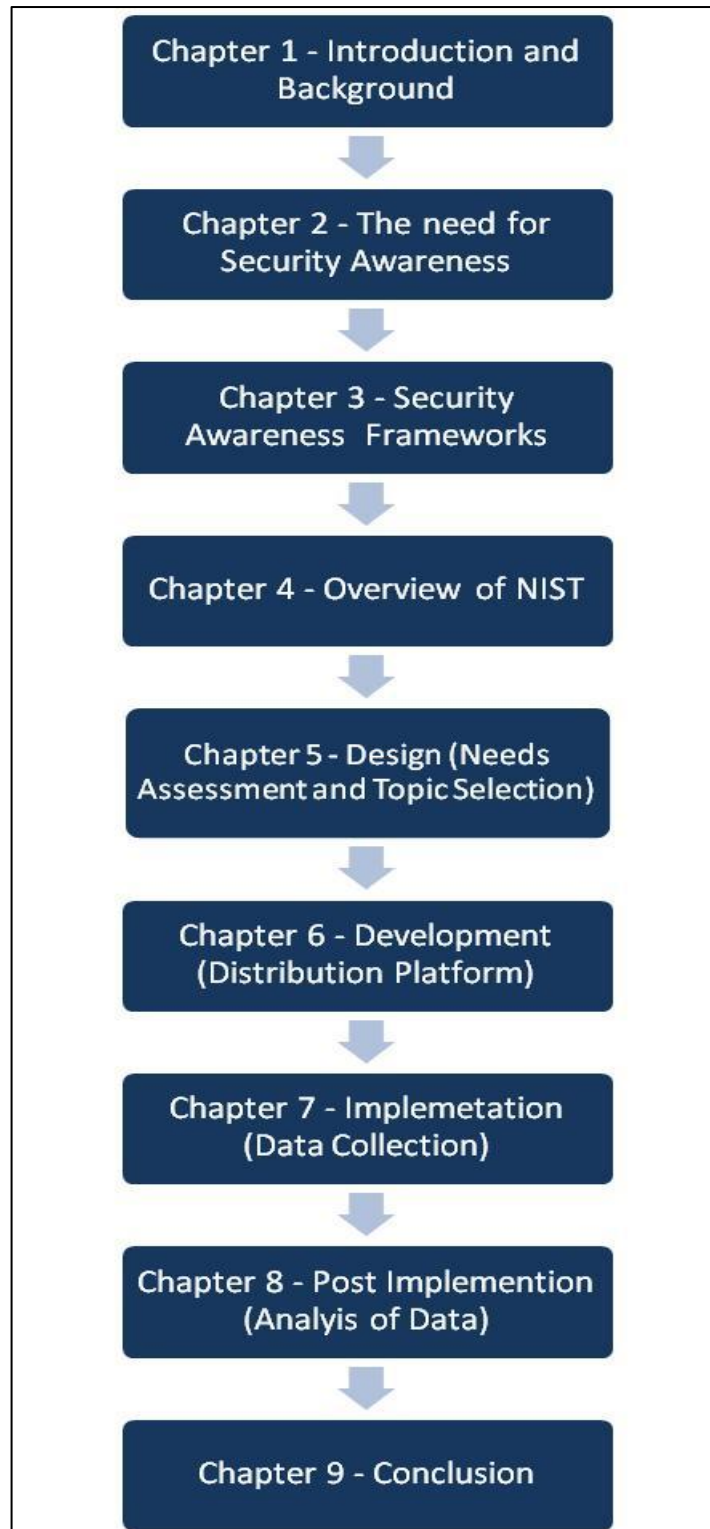
**Chapter 6** describes the high-level design of an autonomous information security awareness system and the requirements for a gaming component to transfer information security awareness knowledge to the player.

**Chapter 7** discusses the implementation of a social networking site to determine the effectiveness of using game play to enhance the retention of knowledge acquired during the information security awareness program.

**Chapter 8** examines the data collected during the game play and describes the findings on the effectiveness during the information security awareness program.

**Chapter 9** concludes by providing an overview of the dissertation as well as highlighting the contribution, limitations and opportunities for future research.

The logical sequence of the dissertation layout is depicted in Figure 1-1.



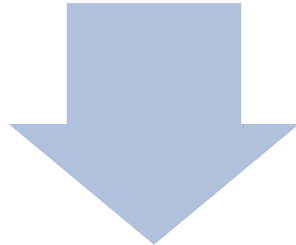
**Figure 1-1: Layout of Dissertation**

The following chapter addresses the importance of information security awareness and describe the concepts associated within the information security awareness domain.



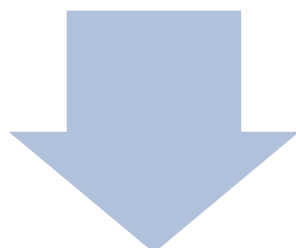
## Chapter 2: Information Security Awareness

Chapter 1 - Introduction and Research Objectives



### Chapter 2 - Information Security Awareness

- 2.1 Introduction
- 2.2 What is Information Security?
- 2.3 Importance of Information Security
- 2.4 Security Controls used within Information Technology
- 2.5 Information Security Awareness
- 2.6 Conclusion



Chapter 3 - Information Security Awareness Program

Figure 2-1: Layout of Chapter 2

## 2.1 Introduction

This literature review chapter provides an overview of the concept of security within the field of Information Technology (IT) and how information security awareness relates to information security. Information security refers to the concept of applying methods to protect items of value from harm or threats which could damage or destroy the item. The protection of the confidentiality, integrity and availability of hardware, software and communication is encapsulated by the concept of information security. Information security awareness provides a paradigm which empowers computer system users with the required skillsets to mitigate threats encountered within the field of IT.

The remainder of the chapter comprises the following sections: Section 2.2 provides the concept of information security as found in literature; Section 2.3 discusses the importance of information security; Section 2.4 elaborates on security controls used within information technology; Section 2.5 introduces the concept of information security awareness and a conclusion is provided in Section 2.6.

## 2.2 What is Information Security?

Information security is defined as the protection of assets (Gollmann 2010). Assets are resources which have value. Examples include but are not limited to credit card details, data, software, personal information, profiles on social networking sites, physical peripherals which include monitors and backup hard drives. Protection is defined as the act to hold something securely or measure implemented to prevent loss (Dictionary.com 2012b). Similarly, Landwehr (2001) describes computer security as making computers safe from threats and preventing users from worrying about the possibility of exploitation. In addition, definitions of 'security' from the online dictionary Dictionary.com include (Dictionary.com 2012c):

- Freedom from danger, risk, etc.; safety.
- Freedom from care, anxiety, or doubt; well-founded confidence.
- Something that secures or makes safe; protection; defence.
- Precautions taken to guard against crime, attack, sabotage, espionage, etc.

Based on these definitions of 'security', the need for protection from dangers originating from cyberspace is also required within the domain of information technology. Therefore

the term security is also applicable to the context of information technology and the term security and information security will be used interchangeably.

Integrity, availability and confidentiality are security principles within information security programs (Harris 2005). Users should be able to always access the requested data (availability) which has not been altered (integrity) and is only readable to them (confidentiality). The importance of these three principles are seen wherever data is used to make critical decisions, for example in military operations where the safety of troops, the national security of a country or the outcome of a war can be adversely affected by crucial decisions made on incorrect data. Coincidentally, the objectives of information warfare are the disruption of these three principles (Libicki 1995). To take another example, an online banking user requires access to their online banking facility any time of the day (availability), only that user should be able to access his/her account (confidentiality), and the information displayed to that user should be correct and up to date (integrity).

In brief, the protection of assets could be achieved by prevention, detection and response: taking measures to prevent assets being exploited, taking measures once it has been detected that assets are being attacked; and taking measures to restore the assets after an attack. For example, the implementation of an information security awareness program, the deployment of anti-virus software, firewalls, and regular updates to the operating system could prevent the computer asset from exploitation by cyberattacks. Installing an information security tool, for example an intrusion detection system, could detect attacks when they occur. Also, the time necessary to recover a computer system after an attack could be vastly decreased by having copies of data stored on external devices.

After this brief introduction to the concept of security, the discussion moves on the importance of security of users of information technology.

### **2.3 Importance of Information Security**

Businesses and individuals are affected by threats, especially within the information technology sector.

Attackers can infect systems either by installing malicious code or by exploiting vulnerabilities in a system. Infected systems can be used in different ways to create profit for criminals. Criminals may use extortion, fraud and spam to make a profit. In the case of ransomware, access to the victim's system is denied once it is infected. The victim has to

pay a ransom to the criminal before access to the system is restored (O’Gorman & McDonald 2012). Extortion may be implemented through a Denial-of-Service (DoS) attack or by the theft of sensitive information from a company and threatening to sell or reveal that information to the public or competitors. Fraud involves the use of phishing attacks to steal information about individuals using an infected system: for example, the use of keyboard loggers to steal credit card details, passwords and other sensitive information (Provos, McNamee, Mavrommatis, Wang & Modadugu 2007).

Social engineering tactics are used to lure unsuspecting users to a website that infects the system with the use of ‘drive-by-download’ malware (2008). Drive-by-download infections occur when a user visits a website that subsequently redirects the user to another web page; this second web page then programmatically attempts to exploit the user’s web browser (Constantin 2014).

Browser hijacking can be used to force users to visit websites that make use of pay-per-click advertising (Polychronakis, Mavrommatis & Provos 2008). Spam is used to send e-mail that advertises products or services to as many users as possible (Stone-Gross, Holz, Stringhini & Vigna 2011). Malware can harvest e-mail addresses from infected systems or create an open relay e-mail service that will send e-mail from the infected system (Joe 2004). This is supported by Stewart (2006) who reported that online crime, for example phishing, spam and extortion, has a link to malware.

Miliefsky (2011) predicted an increase in unknown vulnerabilities from 2011. These unknown vulnerabilities are classified as zero-day vulnerabilities as the security community are not aware of the threat. This forecast was proved to be correct by the discovery of several new zero-day vulnerabilities since 2011. The security company Secunia compiled a report in 2015 which highlights the increase of new zero-day vulnerabilities (Secunia 2015). They reported that 25 new zero-day vulnerabilities were discovered in 2014 compared to the 14 zero-day vulnerabilities discovered in 2013. The following is not an exhaustive list but does indicate an increase of zero-day vulnerabilities:

- Gregory and Glance (2013) conducted a review of information security trends from 2012 to 2013. One trend identified was the increase of malware targeting the Apple platform.

- In April 2014, the Heartbleed vulnerability was discovered in the OpenSSL cryptography library (Zhang, Choffnes, Levin, Dumitras, Mislove, Schulman & Wilson 2014).
- On 24 September 2014, Shellshock was discovered, subsequently allowing attackers to gain access to computer systems (Graham-Cumming 2014).
- Padding Oracle On Downgraded Legacy Encryption (POODLE) was also disclosed in September 2014, allowing attackers to view encrypted messages (Zorz 2014b).
- In October 2014, another zero day vulnerability was disclosed which allowed attackers to embed malware into Microsoft PowerPoint (Zorz 2014a).

Computer threats can be neutralised with the implementation of mitigation techniques. The deployment of software tools such as a firewall and an anti-virus (AV) suite onto computer systems protects against threats. An AV suite protects the computer system against infections by known computer viruses. However, the presence of an AV suite on a computer does not guarantee protection against unknown viruses which are continually under development. This implies a new variant of a virus may not be correctly detected by the AV suite. Another problem is that users are required to update the AV suite's virus database regularly which is impeded by two factors: firstly, they need to remember to update the database, and secondly, the database is usually a large download.

A feasible countermeasure is the promotion of information security awareness amongst users. Goodman, Kirk and Kirk (2007) noted that uninformed users could perform actions that might unintentional infect systems with malware, which in turn provides cybercriminals with resources to fund their underground economy. Many attacks require the user to perform an action that allows malicious software to exploit vulnerabilities within a computer system. However, if the user had prior knowledge about the possible exploitation techniques, he could have employed mitigation techniques learned during an information security awareness program.

Consider the case of a user who opens an email from an unknown sender with an attachment. Cybercriminals could embed malware into attachments and then using an email to deliver the malware to a wide variety of unsuspecting users. Such tactics decreases suspicion from the user receiving the email with the malware (Razzaq, Hur, Ahmad, & Masood, 2013). The probability of exploitation is high if the user is not aware of

this fact and mitigation is left to the AV to provide protection. In the case of the user having attended an information security awareness program that described these exploitation tactics, as well as a mitigation technique, the user could have deleted the email received from this unknown source and thus prevented a possible exploitation without relying on the AV to provide protection.

Also regard the case of users at companies being protected by measures implemented by their organisations. These measures could vary from anti-virus software running on the computers, the use of intrusion detection systems and firewalls, and users attending computer and information security awareness programs. Even users with little computer and information security knowledge are, to a certain degree, protected by measures implemented by their organisations. This means that the computer and information security awareness level of the user could determine if they will be lured into a phishing attack by a well-conceived social engineering attack or have their system infected with malware. Access to the Internet is usually carried out through the use of web browsers (Theobald & Dunsmore 2000). Users would, for example, use a web browser like Google Chrome, Microsoft Internet Explorer or Mozilla Firefox to access research papers, read news articles, to do online shopping, use internet banking, and socialise through social networking. Polychronkis et al. (2008); Cavalca and Goldoni (2008); and Provos et al. (2007) have conducted research on web based malware which indicates that the web browser is the primary vector of system infection. The report by Secunia (2015) disclosed an increase of 42% of vulnerabilities identified across the major web browsers from 2013 to 2014.

Information security could be used to prevent or at least minimise data loss, maintain productivity, guard against cyberterrorism, outwit identity theft and prevent adverse legal consequences (Ciampa 2004).

The following list describes some cybercrimes that occurred between 2011 and 2014. This is not an exhaustive list and merely demonstrates the importance of security pertaining to information technology:

- Cramer (2011) reported on a scam which targeted home users. The attackers used telephonic devices to call victims at home. They impersonated computer security engineers from well-known computer companies, for example Microsoft, as part of their techniques to build trust with the victims. Next the attackers would inform the

victims about risks from one or another computer security threat and provide a free service to mitigate the threat. The attackers convinced the victims of a possible infection that required them to perform remedial actions to fix the problem. These included downloading and installing software from the attacker's website or providing remote access to the victim's computer system. This resulted in unauthorised access to the victim's computer, which allowed the attackers to install additional malware for nefarious purposes like logging credit card details, authentication information and access to personal information.

- An amount of R42m was stolen from the Postbank in South Africa (Swart & Afrika 2012). Prior to this digital heist, the cybercriminals created bank accounts. The criminals waited until the offices of the company closed for the New Year and then used a compromised employee's computer to access the servers and deposit money into their bank accounts. The heist started on the 1<sup>st</sup> of January 2012 and stopped on the 3<sup>rd</sup> of January 2012 when the offices opened for business. The legitimate account holders could not do anything to prevent this from happening; the focus is on the employee whose computer was used to access the server. In a banking environment, all computers require a username and password to access the computer. The employee could have used a weak password, shared the password with a colleague or wrote the password on a paper. All these dangerous practices could be addressed by information security awareness programs to educate users on good password practices.
- The Eurograbber campaign made use of the malware called Zeus to steal an estimated of €36 million from over 30,000 customers across Europe in 2012 (Rashid 2012). Infected users had been lured to visit malicious websites. The malware could steal authentication credentials, which included usernames and passwords, and also intercepted banking sessions. The Eurograbber campaign also targeted mobile devices, including Android, BlackBerry, Symbian and 'jailbroken' iPhone systems.
- In 2013 a series of attacks were launched against diplomatic, governmental and scientific research organisations in different countries. The main objective of this attack was to harvest intelligence from compromised organisations. The attackers

used email as the delivery mechanism to infect the victims' computer systems (Kaspersky Lab 2014).

- In 2014, hackers allegedly illegally accessed Apple services, which included iCloud, resulting in stealing and distributing nude photos of actresses. A flawed security design was bypassed by the attackers to gain access to the victims' accounts. The attackers used a brute force password attack, resulting in access to the accounts (Stanford & Robertson 2014).

An understanding is required to gain knowledge about the different vectors that can be used to target assets. Vectors can be described as the options available to an attacker which could be used to target victims. For example, an attacker could target a laptop through the network, malicious software or physically. Awareness of these attack vectors could assist in mitigating the potential threats (Beaver 2007). These vectors include but are not limited to:

- **Non-technical attacks** – These attacks target the human element using manipulation techniques to lure the person to perform detrimental actions, like providing passwords to attackers or opening a file containing malware and thus infecting the computer system.
- **Network infrastructure attacks** – The majority of devices like computers are connected to wired and/or wireless networks. Users are required to access networking services, for example email to conduct their daily tasks. Attackers target networks in an attempt to disrupt network connectivity as in the case whereby services can be disrupted through a denial of service attack (Schuba, Krsul, Kuhn, Spafford, Sundaram & Zamboni 1997).
- **Operating system attacks** – Computer devices require an operating system to provide the user with the capability to perform several tasks, which include writing a document, watching a movie, or accessing the Internet. Due to the complexity of operating systems, many vulnerabilities exist which attackers attempt to exploit. Vendors issue patches to fix the vulnerabilities, but many users omit to apply the patches, leaving the operating system vulnerable to attack.
- **Application and other specialised attacks** – Attackers know that the latest operating system updates will prevent several exploitation possibilities. However other opportunities still exist. As with operating systems, applications also have



vulnerabilities which can be exploited. Examples of exploitable applications include but are not limited to web browsers (e.g., Mozilla Firefox), word processors (e.g., Microsoft Word) and multi-platform software (e.g., Java and Adobe Flash).

Security vendors have developed tools to address the different attack vectors, subsequently creating a market for information technology security mitigation controls. The following section describes the main security controls implemented by the majority of computer end users which include novice and advance users.

## 2.4 Security Controls used within Information Technology

Many security vendors have developed solutions that address the different information security attack vector these include running an anti-virus package and a firewall. Also advice from security experts recommends updating the operating system regularly. Both the solutions and recommendation are considered as security controls. The combination of these controls results in a secure system however the limitations of these should be considered (Figure 2-2).

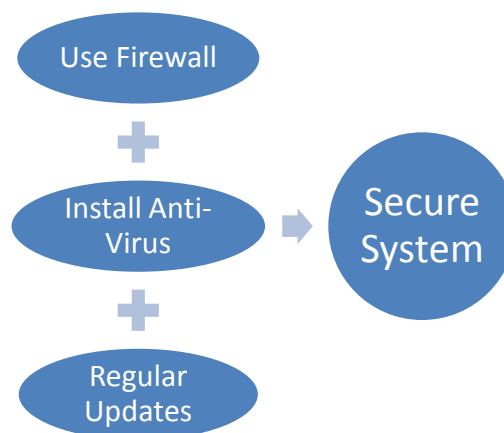


Figure 2-2: Information Technology Security Techniques (Source: Own)

The effectiveness of each of these controls is discussed next.

### 2.4.1 Effectiveness of updates to operating systems

Many users' computer systems require an operating system to function. The operating system consists of software interacting with hardware, for example, the monitor produces results from different inputs like the keyboard and mouse. To elaborate further, the user press a key on the keyboard (input), the operating system recognises the key that was pressed and then interacts with the monitor (output) to display the key which was pressed. However, since the operating system consists of software components, these may have

vulnerabilities that could be exploited by attackers. The typical vulnerability lifecycle for operating systems consist of four points in time. Frei, Tellenach and Plattner (2008) describe these as follows:

- **Discovery Time** – The earliest time for identifying a vulnerability which could be used for exploitation.
- **Exploit Time** – The earliest time attackers could take advantage of the discovered exploit.
- **Disclosure Time** – The time when vulnerability has been analysed by experts and the information about the exploit is freely available to the public.
- **Patch Time** – The time at which the vendor releases a patch to secure the vulnerability.

These types of vulnerabilities are known as zero-day vulnerabilities. The vendor cannot fix a vulnerability if they are not aware of the cause or the location of the security bug. This implies that even if computer operating systems have been patched, there may still be other zero-day vulnerabilities which could be used by cybercriminals to exploit computer systems. This is possible due to the differences between disclosure and patch time. Attackers need to first use the exploit for the security community to become aware of it; the security community then requires additional time to understand the exploit before contacting vendors to develop fixes to mitigate the vulnerability. This implies many systems could already be exploited by the time an update becomes available to the public. Goodin (2012) reported the average disclosure time of a zero-day attack is 312 days. Microsoft releases security patches on the second Tuesday of each month for its Windows operating system (also known as “Patch Tuesday” (Coppens, De Sutter & De Bosschere 2013)). This implies that Windows users have to wait until “Patch Tuesday” before being able to fix the vulnerability in their operating system, even in the event of discovering a critical vulnerability. Furthermore, users still need to install the updates when they become available.

Many operating systems are configurable to assist in the installation of updates. Microsoft Windows users have three options available, which include being notified when updates are available, automatically downloading the updates and prompting the user to install them, and automatically downloading and installing the updates. Users might not be aware

of these options or understand their effect, and could still ignore notices of available updates.

Duebendorfer and Frei (2009) have shown that automated installation of updates improves security. The study used the Google Chrome web browser as the target platform. Google Chrome automatically updates without notifying the user when any new updates become available.

These three issues of disclosure time, development with rollout of patches and user intervention emphasize that even roll-outs of updates to computer operating systems is not always an effective protective measure against a possible attack from cybercriminals.

#### **2.4.2 Effectiveness of anti-virus software**

Anti-virus software has the capability to identify viruses that have already been positively identified by anti-virus vendors (Plant & Murrell 2007). The anti-virus software is installed on the user's computer but must be kept up to date with the newest virus signatures to be effective. Conversely anti-virus software will become ineffective once the update with the newest virus signatures have been completed as new viruses have been created since the release of the virus signatures by the vendors (Nachreiner 2015).

Baggett (2008) conducted a study in 2008 to determine how effectively anti-virus solutions dealt with malicious payloads created by Metasploit. A payload is defined as an exploit encapsulated within a delivery mechanism send to a target (Wikia 2015). The Metasploit Framework provides an open source framework with the latest and most effective exploits to conduct penetration testing (Kennedy, O'Gorman, Kearns & Aharoni 2011). These exploits resemble current threats that have been identified within the cybersecurity community and could exploit systems which have not been updated with the latest patches. The payload consists of software code that exploits a vulnerable system. These payloads were then deployed on target machines running anti-virus software. Moreover, he submitted the samples to Virustotal.com, a free online malicious content analyser used to identify malware, to determine which anti-virus vendors could detect the payloads as malicious. He found that all anti-virus software were ineffective against the payloads created using the Metasploit Framework, which implies users could have a false sense of security by using updated anti-virus software. The ineffectiveness of anti-virus software was again highlighted by Haffejee and Irwan (2014) who demonstrated how anti-virus software could also be evaded.

The Carberp botnet was investigated by McKenney (2011). Although the botnet only consisted of 603 infections, the capabilities demonstrated by the botnet, which in this case included the capability to circumvent anti-virus software, provide evidence of the evolution of botnets. The anti-virus software vendors used during the investigation included Norton360, Microsoft Security Essentials, AVG, Sophos, Kaspersky and Avast. These companies still form part of the leading anti-virus software providers as identified by the OPSWAT software security company (2014). The worrying fact is that all these vendors provide solutions to computer users against the threat of malicious software.

The FireEye Malware Intelligence Lab (2012) provided a report on the threat landscape in 2012. They also included the evolution of advanced malware, tactics used by advanced persistent threats and insight into the level of network infiltration within organisations. They found a substantial increase in advanced malware and bypassing of traditional signature-based security mechanisms.

Imperva (2012), a data security company which specialises in database, file system, and web application security, conducted a study in 2012 to determine the effectiveness of anti-virus software. They also concluded that less than 5% of newly created malware can be detected by anti-virus software developed by vendors from across the globe. Also, some vendors could only provide an effective solution within 4 weeks. These cases highlight the argument that anti-virus solutions cannot be used on its own to protect users against cyberthreats, but should form part of security threat mitigation package.

This section highlighted the ineffectiveness of only using anti-virus software as a security measure against cyberthreats. Other security measures are discussed next and should be used together with anti-virus software to provide a holistic security solution.

### **2.4.3 Effectiveness of firewalls**

Firewalls could be implemented as hardware or software controls that inspect data packets traversing between networking devices. The data packets are inspected against a set of rules and then either discarded or forwarded based on the rule set (Tomsho 2011). A report by Chai (2011) indicated that security tools, including firewalls are only 60% effective if installed with only the default configurations, and in some cases even as low as 20%. The effectiveness does improve to 80% once a security knowledgeable user configures the tools. These findings highlights two problems for home-end users who want to install firewalls on their own:

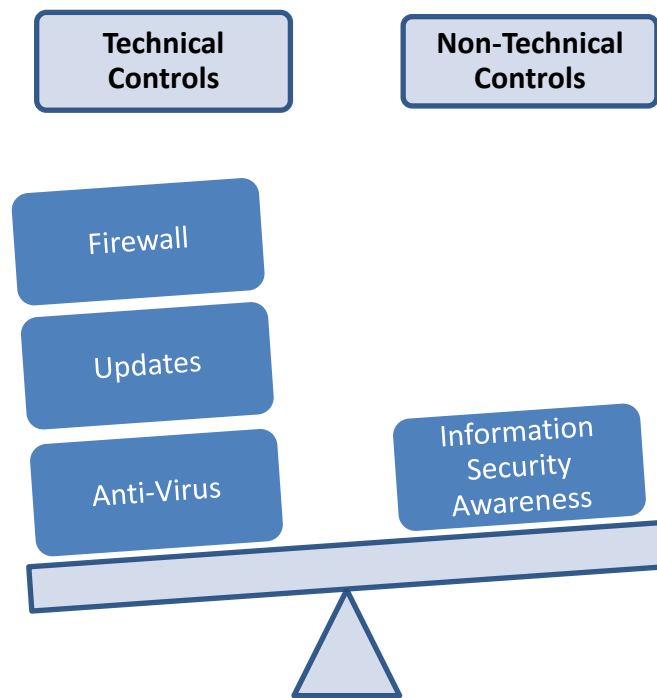
- The first problem is that, once configured correctly, the firewall provides only 80% protection against threats.
- The second problem is not all home-end users have the knowledge to configure these devices.

Both these problems decrease the effectiveness of firewalls. Moreover Fogarty (2011), reported on the effectiveness of the 6 leading firewall systems. Some of the firewalls used in the tests conducted could not process all the requests and became unstable while other firewalls could not prevent network attacks. Also work conducted by Du Zhang, Jujjavarapu and Meiliu Lu (2014) highlighted the creation of conflicting rules as a major cause of inconsistencies found in firewalls which also effects the performance of the firewalls (Wang, Zhang, Lu, Zhao, Zhang & Zheng 2014).

These issues pertaining to firewalls are alarming with respect to securing the home-end user's computer.

#### **2.4.4 Conclusion**

The previous section described the implementation of controls to protect computer users. These controls however can be classified as either technical or non-technical controls, as depicted in Figure 2-3. The technical controls are considered to be tangible and can be implemented without knowledge of the functionality, e.g., firewall software. They also were designed and developed to mitigate technical threats.



**Figure 2-3: Information Technology Security Controls (Source: Own)**

The effectiveness of each of these technical components is refutable and circumspect. Also, technology cannot address an attack vector which is non-technical and focuses on the human element. A report by Davis, Holden, Jagdale, Gragido, Hein and Hills (2011) identified sequential stages executed as part of an attack originating from cyberspace. These stages were identified as lures, redirects, exploit kits, dropper files, call-home communications and finally data theft. The lure stage influences the user to perform an action, for example visit a malicious site. The cybercriminal has to craft inventive methods to increase the likelihood that the unsuspecting user will perform the desired action. These criminals revert to luring the users to click on links specifically designed to attract their attention and influence them enough to click on the link. The ensuing technical stages are automated and can only be initiated by the user who is lured to visit the malicious site. Therefore, all users should be equipped with the required knowledge that would prevent them from being lured into performing these undesired actions. This could be accomplished with the implementation of an information security awareness program which falls under the non-technical security control category.

The use of information security awareness programs is recommended by Wilshusen and Lawrence (2011), who reported on how federal agencies information systems in the United States of America are at risk. They attribute this high risk to insufficient training of

personnel with regards to information security policies. Security breaches occur as a result of actions by ignorant users which can be addressed by equipping users with enough knowledge to mitigate the threats encountered (Colón 2014). Security knowledge can be transferred to users by means of information security awareness programs, which is addressed in the next section.

## **2.5 Information Security Awareness**

### **2.5.1 Definition**

Information security awareness, according to Wilson and Hash (2003), is not training but the focussing of attention on Information Technology (IT) security concerns and empowering people to respond accordingly. It is becoming increasingly important for all users, and not just technical staff, to be aware of safe cyber practices. Eminağaoğlu et al. (2009) stated that not only technical security training of IT staff, but also information security awareness training and other awareness campaigns have become a “must” for everyone. Many users are ignorant of the range of threats spanning cyberspace and the Internet. By using cybersecurity campaigns, also known as information security awareness programs, awareness of current threats can be created, as well as educate users on best practices to identify and handle threats. Home users could also benefit from such information security awareness campaigns that warn them of the latest threats or provide useful tips on safe internet surfing. Kritzinger and Von Solms (2010) state the vulnerability of personal Internet users is due to the fact that they lack the information security knowledge to understand and protect their personal computer (PC) and therefore also their personal information.

Awareness, according to the Oxford dictionary (2012), is defined as knowledge or perception of a situation or fact. It is therefore critical to increase the awareness of users whom frequently use computer devices for everyday life, to understand the threats that they can encounter and what techniques can be used to mitigate these threats.

### **2.5.2 Case Study**

In 2004, the University of Missouri – Columbia (MC) implemented an information security awareness program within the university (2004). The awareness program was implemented by conducting monthly activities around a theme, for example password security. The implementation also included in-person and online training. McCoy and

Fowler (2004) discussed the lessons learned from the information security awareness program and identified goals which are important to information security awareness programs. These goals are described as follows:

- Influence the participants of the information security awareness program to result in a positive behaviour change
- Develop and deploy metrics to measure the success of the information security awareness programs
- Implement strategies to ensure a lasting effect of the information security awareness program

They also found that such a program needs to be flexible since not all the users have the same learning styles. The security landscape is also changing rapidly and provision should be made to ensure the content remains relevant.

### **2.5.3 Outcomes**

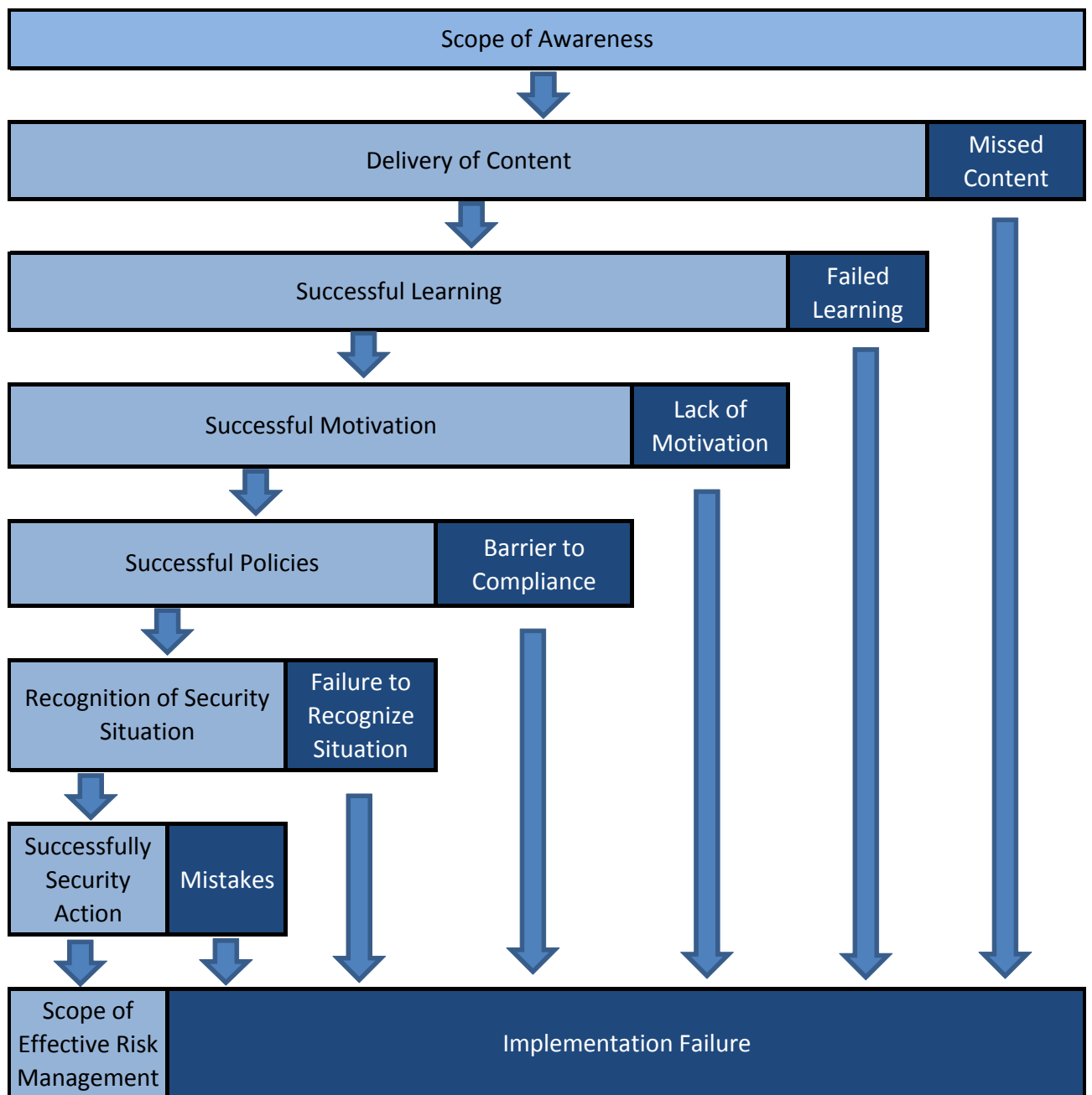
Information security awareness programs can only be seen as having value for the business or individual if awareness levels have increased and positive behaviour is demonstrated, for example the use of strong passwords. Stewart and Austen (2009) described how psychology and marketing can be used to improve the effectiveness of information security awareness programs. Using psychology could be beneficial in promoting positive behaviour by rewarding good actions performed by the users within the organisation. Many information security awareness programs focus on fear as a motivator, which due to the “Boomerang Effect” could decline the impact of such programs (Mann & Hill 1984). In other words, the effectiveness of the information security awareness programs declines instead of increases. Furthermore, users could interpret the same content in different ways, which will affect the goal of the program; it would be beneficial to ensure that all the participants have the same lexicon at the start of these programs in order to avoid this. Stewart and Austen (2009) also indicated that effectiveness could be increased by using marketing tactics, which include understanding the audience and making a call to action which could be measured. Hence, defining a metric could be used to determine the effectiveness of the information security awareness program.



#### **2.5.4 Point of Failure**

In addition, Stewart and Austen (2009) provided a model to show all the points of failure that could influence the outcome of an information security awareness program (Figure 2-4).

The model highlights that the effectiveness could be influenced by the delivery method used, since some content might be missed during the training session due to a wandering mind. The person might not understand the content, which in turn would affect the learning outcomes of the content. Learning could also further be influenced by motivation. It could happen that the person has personal problems that impair learning. In addition, the person might not understand the security policies and how the content correlates with prescribed rules set by the business.



**Figure 2-4: Point of Failure Model (Stewart & Austen 2009)**

The person might also not be able to recognise the security situation due to lack of knowledge. All these components have an effect on the effectiveness of an information security awareness program. Also the “Point of Failure” model identifies several causes of ineffective information security awareness program. Each of these causes should be considered during the development of information security awareness programs. The importance of successful learning is highlighted in the “Point of Failure” model which forms the premise of this dissertation.

The high-level components of information security awareness programs have been identified through a literature study including the work done by McCoy and Fowler (2004). Also, the work described by Stewart and Austen (2009) provides insight in areas which can affect the effectiveness of information security awareness programs. These are important points to take into consideration for implementing successful information security awareness programs as well as improving existing programs. Information security awareness program design and development methodologies are described in Chapter 3.

## **2.6 Conclusion**

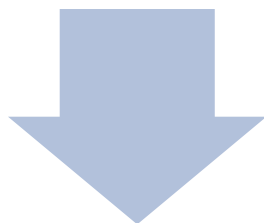
This chapter addressed the need to understand the concept of information security and how information security awareness is an integral part within the information security domain. Many examples of security incidents exist and in most of these cases, the causes are traced back to users who are not aware of the consequences of their actions and also do not have an understanding of the threats encountered within the security domain, especially the Internet.

This chapter identified the need for information security awareness training as a proactive measure to protect against threats that can be encountered by end users. The need for information security awareness programs is further supported by the case studies described in Chapter 5, which highlight the real threats encountered through social media, once incompetent and ignorant users start using these platforms. In addition, this chapter provided a high-level understanding of the different components of an information security awareness program and provided critical points which could influence the effectiveness of such programs. These concepts will be described in greater detail in the next chapter.



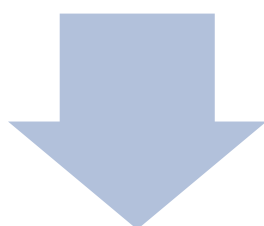
## Chapter 3: Information Security Awareness Program

Chapter 2 - Information Security Awareness



### Chapter 3 - Information Security Awareness Program

- 3.1 Introduction
- 3.2 Standards addressing Information Security Awareness
- 3.3 Information Security Awareness Frameworks
- 3.4 European Union Agency for Network and Information Security (ENISA)
- 3.5 SANS Security Awareness Roadmap
- 3.6 National Institute of Standards and Technology (NIST) Security Framework
- 3.7 Selection of Information Security Awareness Framework
- 3.8 Conclusion

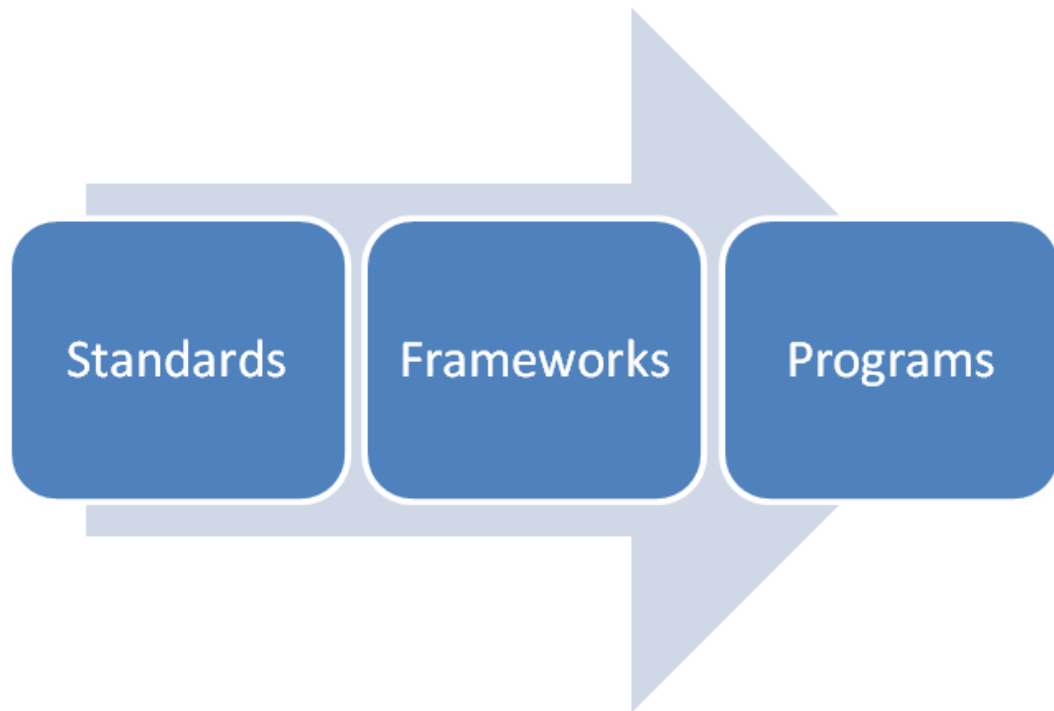


Chapter 4 - Using NIST within an Information Security Awareness Program

Figure 3-1: Layout of Chapter 3

### 3.1 Introduction

The previous chapter addressed the key concepts and the need for information security awareness. Numerous information security awareness frameworks exist, and this chapter will give an overview of three existing frameworks. The role of international standards within these frameworks ensures a common model for implementation. Figure 3-2 shows the relationship between security standards, frameworks and programs.



**Figure 3-2: Relationship between Standards, Frameworks and Security Programs**  
(Source: Own)

Companies are required to adhere to standards applicable to the business sector in which they operate, for example credit card companies are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) (El Kharbili, Stein, Markovic & Pulvermüller 2008). The relevance of standards to information security awareness is briefly described in this chapter as information security awareness programs would fall under these implemented standards. In addition, the identification and selection of an information security awareness framework will be discussed. Several frameworks are used within the context of information security awareness and an understanding of the most commonly used frameworks is required. Subsequently, the background information assimilated during this literature review process is beneficial in the identification and application of a framework within this research context. Thus, the use of standards as part of information

security awareness, together with the identification and selection of an information security awareness framework, is addressed in this chapter.

### **3.2 Standards addressing Information Security Awareness**

It is important in the context of information security awareness to ensure that standards are followed. This will guarantee that a certain level of quality is achieved. A standard is defined by Oxford Dictionaries (2014) as “*Something used as a measure, norm, or model in comparative evaluations*”. It is therefore important to ensure from a feasibility point of view, that funds spent on information security awareness in an organisation achieve the desired outcome of a security conscious culture and results in changes in behaviour that reduce security incidents. Also, the correct and full implementation of standards within organisations would therefore contribute to their compliance. This could be important when companies are evaluated during audits and possible business collaboration, for example before “Company A” can outsource work to “Company B”, “Company B” needs to comply with required security standards. Several standards are available in the information security awareness domain, for example International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC) 27002 (Humphreys 2007), European Union (EU) Data Protection Directive (Birnhack 2008), Federal Information Security Management Act (FISMA) (Hulitt & Vaughn 2010), and Payment Card Industry Data Security Standard (PCI DSS) (Morse & Raval 2008). The mentioned standards are not an exhaustive list. It should also be noted that information security awareness is usually only a subset defined within these standards.

Information security awareness programs form part of all types of business endeavours which are dependent on information technology. The development of standards for specific domains was actualised by the Health Insurance Portability and Accountability Act (HIPAA) of the United States of America (USA). In 1996, this act was signed into American law to protect the privacy of individually identifiable health information (Dwyer III, Weaver & Hughes 2004). Paragraph 164.308(a)(5)(i) within the act defines the topic of information security awareness programs within the organisation. This act specifically addresses the use of “*information security reminders*”, “*having policies which address the protection, mitigation and reporting of malicious software*”, “*password management*” and “*authentication audit to monitor login attempts*”.

With the proliferation of credit card usage as a means to conduct financial transactions, an increase in threats targeting credit cards was noticed. As a result of criminal activities, standards were also developed to protect the credit card industry against credit card fraud and this initiative was defined by the Payment Card Industry Security Standards Council (A. Shaw 2009). The standard consists of six control objectives, which include the implementation of an information security awareness program under PCI DSS Requirements 12.6. This requirement stipulates that an information security awareness program should be implemented and verified for completeness, participation and accessibility (PCI Security Standards Council 2010).

The ISO/IEC 27002 (International Standards Organisation 2012) consists of 114 controls, which each individually address a specific information security requirement identified via a formal assessment. The controls under the ISO/IEC 27002 standard are defined as a recommendation and not a requirement. “*Ownership of assets*”, “*Addressing security in third party agreements*”, “*Controls against malicious code*” and “*Clear desk and clear screen policy*” are examples of such controls. Paragraph 8.2.2 defines the control “*Information security awareness, education, and training*”, which address information security awareness programs.

These standards form part of policies which once implemented, ensure that the company is compliant to a set standard. The controls defined in ISO/IEC 27002 (Paragraph 8.2.2) and HIPAA (Paragraph 164.308(a)(5)(i)) may guide the deployment of an information security awareness training program within a company. An information security awareness training program is designed, developed and deployed by selecting the appropriate information security awareness framework which is best suited to the target environment.

The next section describes the information security awareness frameworks considered for this dissertation. The chapter concludes with the selection of an information security awareness framework to be implemented in the information security awareness program used within this study.

### **3.3 Information Security Awareness Frameworks**

The previous section described the importance of using standards as a mechanism to attain quality within an organisation. Most of the standards defined within an information technology environment require information security awareness training as a control to ensure the employees are equipped to deal with potential cyberthreats. The information



security awareness frameworks developed by the following organisations are described in the following sections:

- European Network and Information Security Agency (ENISA) (Section 3.4)
- SysAdmin, Audit, Networking and Security (SANS) (Section 3.5)
- National Institute of Standards and Technology (Section 3.6)

Other information security awareness frameworks do exist but were not considered, as the comparison between the three selected frameworks provides sufficient insight into the design, development and deployment processes required for an information security awareness program.

In the following sections, each of these frameworks is analysed, and each section concludes with observations regarding potential benefits and drawbacks. The resulting conclusion provides information about the selection process of the framework to be used in this study (US Government Organization 1996).

## **3.4 European Network and Information Security Agency (ENISA)**

### **3.4.1 Overview**

The European Network and Information Security Agency compiled a guide in 2008 on how to raise information security awareness, and released an updated version in 2010 (ENISA 2010). The guide consists of three processes to be used for the development of an information security awareness program. These processes are depicted in Figure 3-3, and are defined as follows:

- **Plan, Access and Design** – Information security awareness programs need to be planned to achieve the required goals. The goals can be achieved by developing achievable and effective modules as specified by the stakeholders.
- **Execute and Manage** – The impact of the information security awareness program can only be achieved by implementing the modules and ensuring resources are available to oversee the execution of the information security awareness program.
- **Evaluate and Adjust** – The effectiveness of an information security awareness program can only be determined by monitoring the impact of the program and evaluating which modules produced the most impact, while subsequently addressing the ineffective modules.

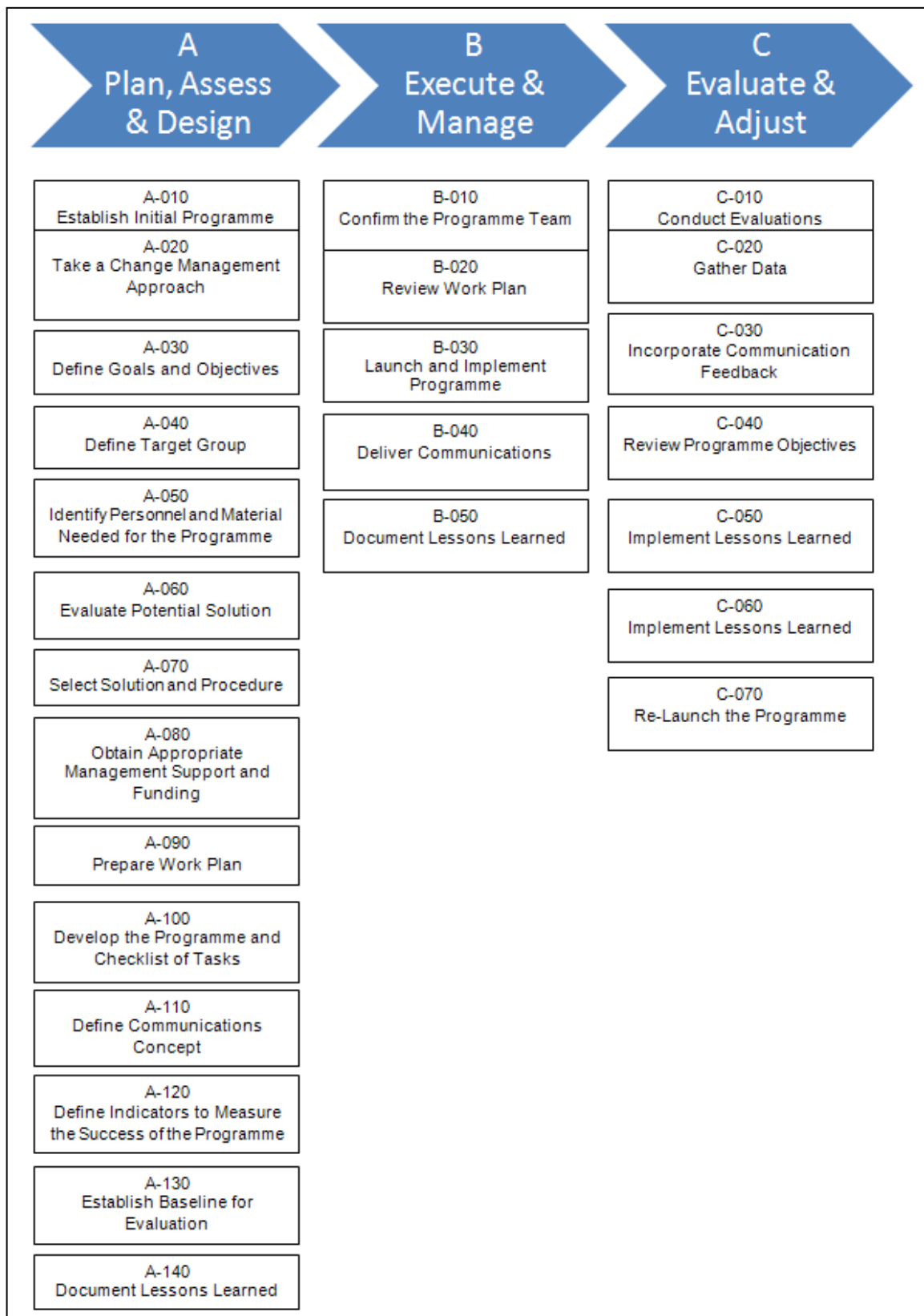


**Figure 3-3: ENISA Information Security Awareness Processes (ENISA 2010)**

Each of these processes consists of sub-processes, which define the steps to be completed to achieve the main process. For example the “*Execute and Manage*” process consists of 5 sub-processes: “*Confirm the Programme Team*”, “*Review Work Plan*”, “*Launch and Implement Programme*”, “*Deliver Communications and Document Lessons Learned*”.

All these sub-processes are used to execute and manage the information security awareness program. However, each sub-process consists of activities, which produces a measurable result. For example, the sub-process “*Establish Initial Programme Team (PT)*” includes, but is not limited to the following activities: “*Develop PT Strategic Plan and Objectives*”, “*Establish Recruitment Strategy and Sources*”, “*Develop Selection Criteria*”, “*Analyse and Create Job*” and “*Post Job*”.

The next section describes the different processes, sub-processes and activities identified within the ENISA guide. The entire guide is depicted in Figure 3-4.



**Figure 3-4: European Network and Information Security Agency Framework (ENISA 2010)**

### **3.4.2 Plan, Assess and Design**

The first process "*Plan, Assess and Design*" defines the sub-processes required to design an information security awareness program based on the needs from the stakeholders. This process entails planning in order to achieve the goals of the stakeholders.

The first step "Establish an Initial Program", numbered A-010 in the ENISA Security Framework (Figure 3-4), entails the identification and recruitment of an information security awareness program team who will be responsible for the initial execution of the program (i.e., to start the project). The development of selection criteria is useful to ensure the best fit candidates are recruited; in addition, processes should be in place to manage expectations from the recruited people, including physical reallocation.

Information security awareness program effectiveness requires changes in behaviour, which may result in resistance from some participants. The use of a change management approach should be a proactive measure to address this resistance to change. The target group will move through different phases, from awareness to commitment, as they become familiar and understand the purpose of the information security awareness program. This can be achieved by providing the target group with information on the topic of interest. This is then followed by having dialogues in the form of workshops to foster understanding, and finally by having interactions that promote secure behaviour. If the preceding steps mentioned were successful, then the target group may commit and support the initiative.

It is important to identify the main purpose of the information security awareness programs once the initial project team and target group has been secured. This could be achieved by identifying any current information security awareness program deployed within the company and determine what security policy needs have been addressed. In addition, clarity should be obtained on the purpose and feasibility of the proposed information security awareness program.

With clear objectives and goals identified, the next step is to define the target group. The target group is seen as the participants of the information security awareness program. Understanding the target group influences the design of the information security awareness program, as the individual members of the target group may be at different knowledge levels on the topic, or may learn using contrasting styles. A baseline of the current information security awareness level of the target group needs to be determined

before executing the program, as this can identify potential problematic areas that need to be addressed by the information security awareness program.

The initial program team are responsible for putting the first components in place (define goals, define objectives, and identify the target group). Next, the personnel to present the program and the material for the program need to be identified and selected. The target group and objectives dictate the personnel and the content of the material. For example, if the objective of the information security awareness program is to train and educate technical personnel, more technically inclined personnel would be selected to present the program. Furthermore, the content of the material should be aligned to the program objectives and the composition of the target group: this material could be obtained from external suppliers if the topics identified are already well-known. New material should be developed if topics covered in the program are new or specific to the organisation. A short list of potential suppliers of the training material should be compiled if the material is not going to be developed internally.

Once the material has been identified, the source to provide the material needs to be selected. If the material is to be developed internally, it could impact the implementation time and cost (for example, more team members may need to be hired). Alternatively, the material could be procured from external sources.

Once the solution has been selected, the selected provider should be contacted to clarify aspects including training material content, budget, terms and timeframes. The timeframe impacts the delivery of the information security awareness program as the material forms an essential part of the program. Also, if the material is not affordable, an alternative solution provider needs to be identified as this too can impact the delivery time.

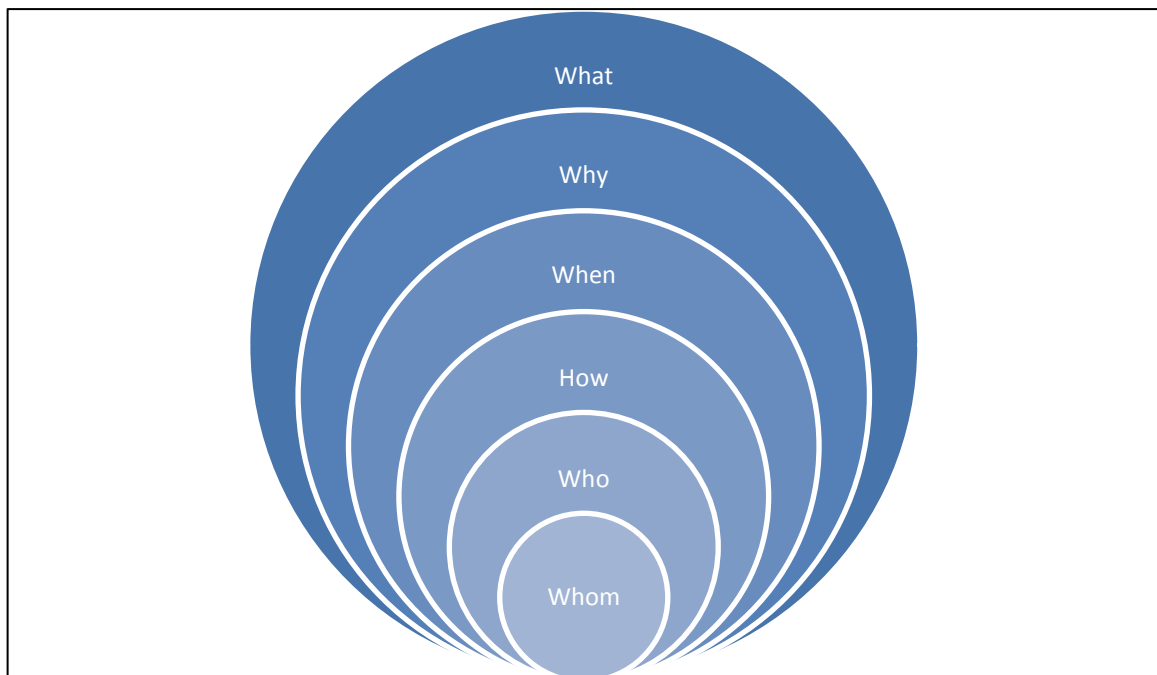
Once enough information is available about the required budget, support and funding also needs to be obtained. Support from influential stakeholders could assist in the process to obtain funding required for the information security awareness program. The use of a formal business case, also known as cost-benefit analysis, shows quantitatively and qualitatively the benefits of the awareness program to management, who ultimately needs to approve the budget before the program can commence.

At this stage, a target group can be identified to participate in the selected information security awareness program, which includes the material and the personnel to conduct the program. Importantly, the program must have an approved budget and buy-in from the

relevant stakeholders. With all these components in place, the next step is the preparation of a work plan to identify the main activities, resources, timelines and milestones. This work plan does not focus on the detail, but specifies which activities must be completed within designated timeframes, and allocation of duties.

With the high level plan in place, the next step is revising the work plan with more information, for example planning in detail which information security awareness topics would be completed in the most effective manner so as not to confuse the target group. If too many dissimilar topics are presented at the same time, the possibility exists that little knowledge would be transferred due to lack of focus on a particular topic.

The information security awareness program should be communicated to the intended target group using different channels such as posters, videos, screensavers, email and newsletters. A critical component of the program is the delivery of the content to the group: the communication plan describes which channels would be used. Figure 3-5 depicts the basic components of a message, which enhances the potential of the identified audience to engage successfully in the information security awareness program.



**Figure 3-5: Basic Communication Components (ENISA 2010)**

In addition, the effectiveness is also increased by selecting the most suitable communication channel; understanding the intended audience using target group analysis; and selecting the topic(s) most critical to the organisation.

Mechanisms also known as security metrics need to be put into place before the start of the information security awareness program to determine the effectiveness of the program when completed. Jaquith (2007) described good metrics should be consistently measured, cheap to gather, expressed as number or percentage and expressed using at least one unit of measure. Examples of metrics are “Number of events listed per month”, “Number of people attending training”, “Number of unique visitors to website” and “Number of incidents reported”.

The first process of the ENISA information security awareness, which addresses planning, assessing and design of the program, concludes with a ‘lessons learned’ session to capture feedback on the steps taken, which could be used to improve future programs.

### **3.4.3 Execute and Manage**

The second process “*Execute and Manage*” focuses on executing the proposed information security awareness program. As the first process focused on establishing the components required for the information security awareness program, this process puts the plan into effect.

Before launching the information security awareness program, the team needs to be confirmed, as they will be responsible for executing and managing all the events planned. Each team member needs to be briefed about responsibilities and communication channels to ensure information flows between the team members and stakeholders.

The work plan also needs to be reviewed following the confirmation of the team. Due to possible changes after the initial undertaking on the work plan, all items including the milestones and budget could be revised and updated if required.

The information security awareness program launches once the team and the work plan has been finalised. The required material is either procured or developed and subsequently then delivered to the target group through the selected communication channels.

After the completion of the information security awareness program, lessons learned during the “*Execute and Manage*” process should be captured to improve future programs. For example, a lesson learned could be that one of the communication channels used during the particular program was not effective due to certain unforeseen circumstances. Hence, if future requirements are similar to the current program, then the original

communication channel would not be as effective and an alternative should rather be used.

#### **3.4.4 Evaluate**

The last process of the ENISA information security awareness guide is to evaluate the effectiveness of the information security awareness program and make the necessary adjustments for any further programs based on the results from the data captured, provided that the program is not suspended once the first iteration is completed.

Different methods can be used to collect data, including surveys, audits and interviews, which subsequently can be used to determine the effectiveness of the information security awareness program. A typical example is using a survey before and after the program to determine the awareness levels of the target group. The data needs to be analysed once the collection is completed.

The analysed data and other results should be communicated to all the relevant stakeholders and also used to assess the current information security awareness program and make necessary improvements for any future programs. The programme objects should be reviewed with the available results and used together with the lessons learned to adjust the program appropriately.

If planned for, the program can be revised with the lessons learned during the previous program. The information security awareness program can then be re-launched.

#### **3.4.5 Evaluation Result of ENISA Information Security Awareness Framework**

The previous sections summarised the information security awareness framework developed by ENISA. This framework is comprehensive and ensures that future programs would be more effective, due to the capturing and incorporation of lessons learned during the execution of the current information security awareness program. The sequential steps of the framework are intuitive and provide important milestones which can be measured. The milestones also provide feedback on progress within the processes defined by the ENISA information security awareness framework. However, a possible drawback of this framework may be the time needed to implement an information security awareness program. In larger organisations, the process to get the required buy-in from the decision makers could restrict the potential of the ENISA information security awareness framework.



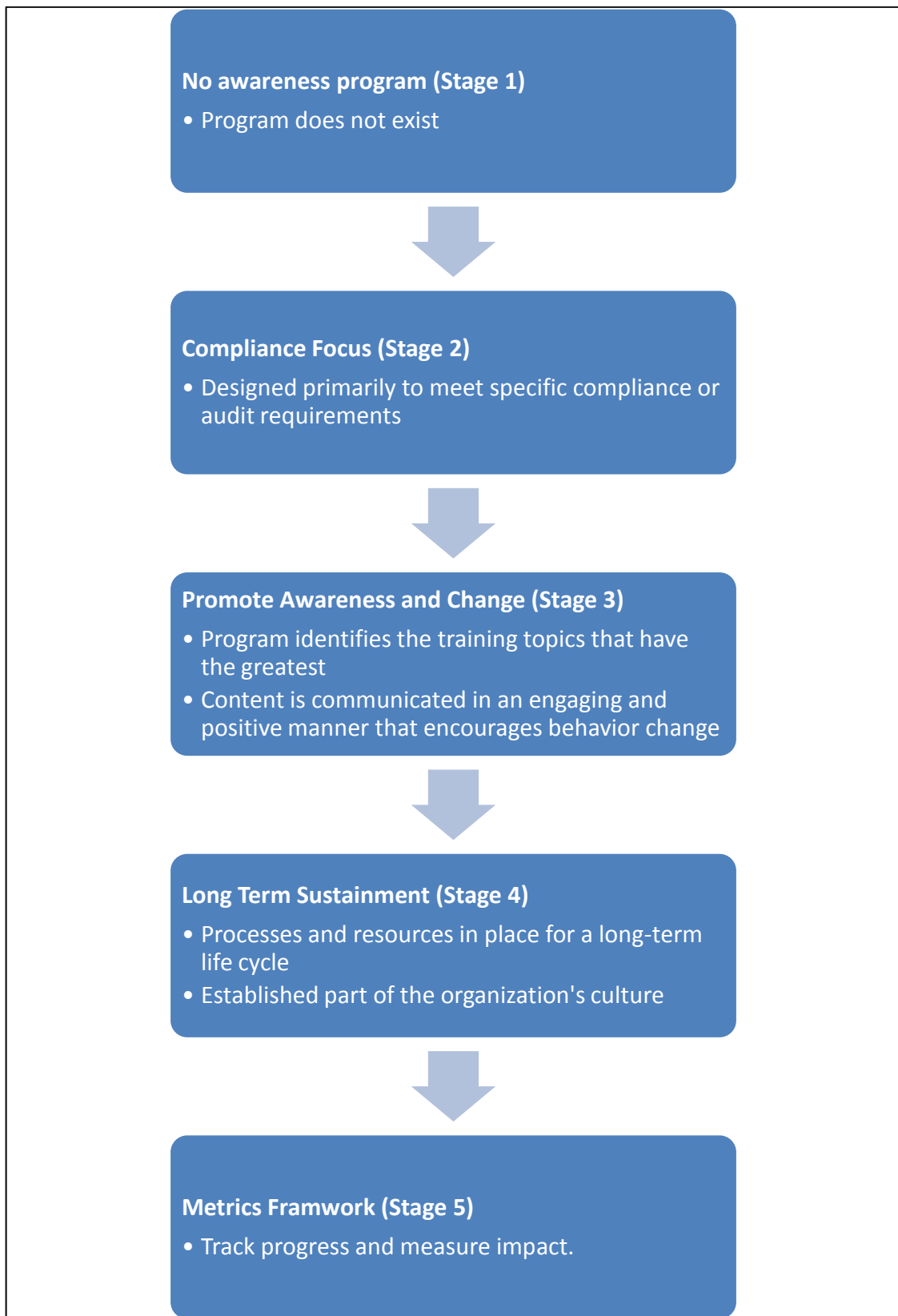
The SysAdmin, Audit, Networking and Security (SANS) Information Security Awareness Roadmap is analysed in the following section.

## **3.5 SANS Information Security Awareness Roadmap**

### **3.5.1 Overview**

The roadmap defined by SANS for information security awareness provides the same end-result as the ENISA information security awareness framework, namely the design, development and implementation of an information security awareness program. A roadmap is defined as sequential steps to be completed to obtain a result (Merriam-Webster 2014b). A framework is defined as “*a set of ideas or facts that provide support for something*” (Merriam-Webster 2014a), and hence the implementation of a process should result in a predictable outcome. The outcome from a “framework” and a “roadmap” subsequently produces both a predictable result.

The SANS roadmap is depicted in Figure 3-6 and graphically illustrates the progression from having no awareness program to sustaining the awareness program within the organisation. The roadmap follows five sequential stages: Stage 1 (No awareness program), Stage 2 (Compliance Focus), Stage 3 (Promote Awareness and Change), Stage 4 (Long Term Sustainment) and Stage 5 (Metric Framework). Most organisations develop policies that employees need to follow to ensure that the organisation complies with adopted standards. Policies could, for example, address the number of leave days an employee can use within a year, define the duties and responsibilities of an employee or adherence to work schedules. The company's policies would be used as a guideline to design and develop the information security awareness program. In other words, the content of the policy, which drives compliance in the company, would be reflected by the information security awareness program. The key decisions to be made during this step are the identification of the compliance standards as described, the decision to develop or procure the information security awareness training material and track the progress of the participants.



**Figure 3-6: SANS Information Security Awareness Roadmap (SANS 2010)**

As part of the SANS roadmap, supporting documents are provided to guide the information security awareness developers at each stage. The documents for each stage are listed in Table 3-1.

**Table 3-1: SANS Supporting Documents**

Document Name	Document Name
Stage02-01-ComplianceRequirements.docx	Stage03-06-TopicsMatrix.xlsx
Stage02-02-SecurityAwarenessPolicy.docx	Stage03-07-LearningObjectives.docx
Stage03-01-StakeholderMatrix.xls	Stage03-08-ExecutionPlan.docx
Stage03-02-GainingStakeholderSupport.pptx	Stage03-09-Checklists.xlsx
Stage03-03-HumanRiskSurvey.docx	Stage04-01-ContentTrackingMatrix.xlsx
Stage03-04-ProjectCharter.xls	Stage05-01-MetricsMatrix.xlsx
Stage03-05-SteeringCommitteeMatrix.xls	Stage05-02-PhishingAssessmentPlan.docx

Note that no documents are associated with the first stage (Stage 1), as no awareness programs exist. The information security awareness program is initiated by the documents named in “*Stage02*”. Some of the documents that form part of the SANS roadmap are discussed next.

The supporting document, “*Stage02-01-ComplianceRequirements.docx*”, would be used to describe the compliance requirements and could be used to justify the information security awareness program to various stakeholders. It is imperative to have stakeholder buy-in for the program, as it will have a financial impact on the bottom-line of the company and could also affect the productivity of the participants. “*Stage03-08-ExecutionPlan.docx*”, describes the purpose, scope, policy and enforcement of the information security awareness program. These documents are freely available and can be downloaded<sup>1</sup>.

The next step is the design and development of training topics to form part of the information security awareness program. The selection of the training topics would be conducted as part of the design and development phase. These training topics could be communicated to the participants of the information security awareness program through various channels, including screensavers, posters, computer based training (CBT), in-person training, games or group discussions. The objectives of the information security awareness program would be achieved when the behaviour of the participants changes due to the positive impact of the knowledge captured within the topics. Some examples of positive change could be observed when the participants of the information security

---

<sup>1</sup><http://www.securingthehuman.org/media/resources/planning/STH-RESOURCE-AwarenessPlanningKit.zip>

awareness program log out of their computer workstations when they leave the office, or use complex passwords after attending the training.

The involvement of stakeholders would also be required at this step. They provide the required funding and also assist in other processes required to make the information security awareness program successful. For example, staff would be required to attend the training. The supporting documents at this step capture stakeholder information, present the need for the information security awareness program, contain a preliminary risk survey to provide a high level picture of the current risk in the company, as well as showing the need for an information security awareness program, and finally provide a project charter describing funding, scope, objectives, milestones, assumptions and constraints. The project charter also encapsulates the final decision to support the awareness program and approve the project. The deployment and execution steps of the information security awareness program can only be completed with formal approval.

The next step assures the long-term sustainability of the information security awareness program. This can only be achieved when information security becomes part of the organisation's culture and if participants repeatedly attend awareness programs. The advantages of this are two-fold:

- Ensure knowledge is current to mitigate the latest threats when encountered.
- Knowledge is retained longer when the participant is repeatedly exposed to the same information.

An iterative process needs to be followed to obtain feedback from stakeholders (including the review of participants' feedback), as well as assessing all the topics for relevance (due to the rapid growth of technology over time). It would also be important to review the awareness levels of the employees of the organisation. The supporting documents list the status of each topic and provides ownership and action information. Action information defines the changes to be implemented: for example, updating content on a topic due to the change in technology.

The final step is to have a platform in place for collecting information which continuously measures the information security awareness levels in the company. This could help identify potential areas of concern and measure the effectiveness of the deployed information security awareness program. The measuring platform collects data from

various metrics and examples of information security awareness metrics are listed in Table 3-2.

**Table 3-2: Example of Information Security Awareness Metric Table**

Metric Name	What is Measured	How is it measured	When is it Measured	Who Measures	Details
Training Completion	How many people completed the training material	Reports from online training system	Monthly	Security Team	Online training material covering relevant information security awareness topics
Reading newsletters about latest security-related events	How many people reads articles on information security awareness	Reports from Newsletter System	Weekly	Security Team	Weekly newsletter is distributed to employees to read.
Quizzes	What is the current information security awareness levels	Online quiz	Every second week	Security Team	Quizzes are sent to employees to answer.

The supporting documents list a metric matrix (“*Stage05-01-MetricsMatrix.xlsx*”) which could be used within a company, but it needs to be customised to the company’s environment.

### 3.5.2 Evaluation Result of SANS Information Security Awareness Framework

The SANS information security awareness roadmap provides a high-level description of what is required in each step with additional supporting documents to record information such as approved decisions with each milestone. The supporting documents are customisable for different environments and are merely a guideline of what needs to be achieved at each milestone or stage.

An advantage of using this roadmap is that the design and development of the awareness program are based on information security awareness standards and use metrics to measure the effectiveness of the information security awareness program. This provides a detailed view of the information security awareness levels within the organisation. The implementation of metrics as part of the SANS information security awareness roadmap could be adapted and applied within a customised information security awareness program.

A potential drawback of the SANS roadmap is the possible decrease of effectiveness in an agile environment. In other words, some information security awareness programs do not need to have formal platforms to approve decisions. Such organisational structures are flat and do not have many management layers which aid with prompt decision making. Highly structured environments require stakeholder buy-in and formal approvals via formal documents, including project charters. This could delay the implementation of the program within the organisation. However the SANS roadmap implementation time is shorter than the ENISA information security awareness framework.

In the next section the NIST framework is discussed.

### 3.6 National Institute of Standards and Technology (NIST) Security Framework

#### 3.6.1 Overview

The National Institute of Standards and Technology (NIST) have developed a framework that aims to guide the development of an Information Technology (IT) security program (2003). The NIST framework consists of four high-level steps. Figure 3-7 shows a summary of the relevant steps of the NIST framework to guide the development of an information security awareness campaign. A short summary explanation of each step follows.

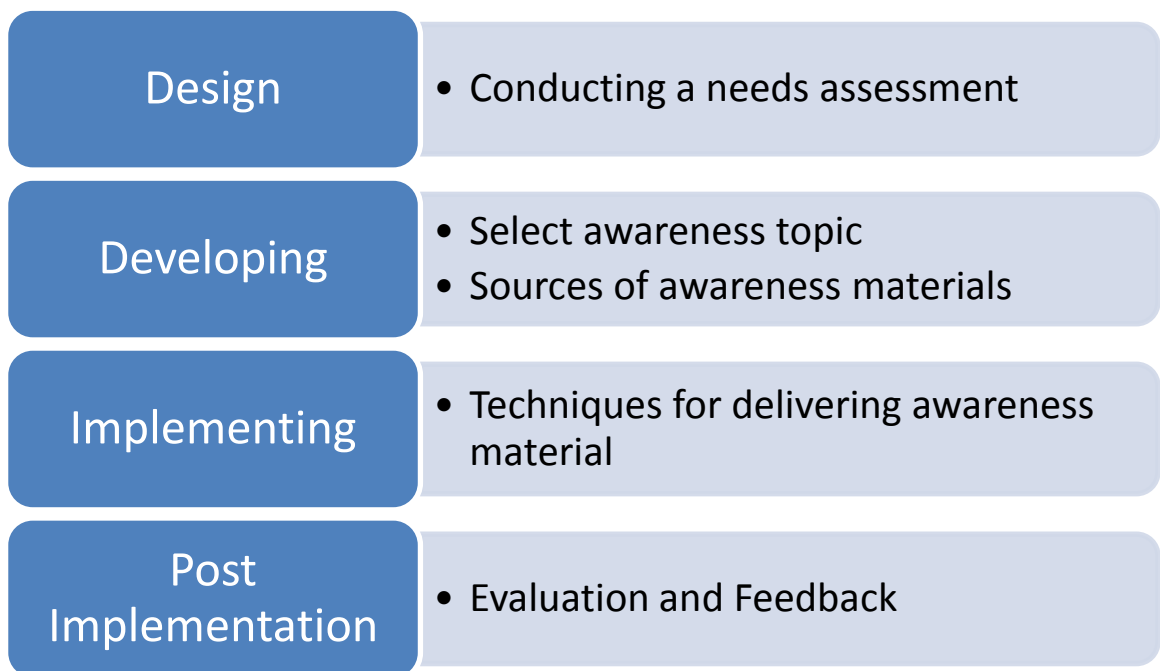


Figure 3-7: NIST Framework (2003)

The first step of the NIST framework is the design phase, whereby a needs assessment is conducted. The needs assessment establishes what the needs of the organisation are in terms of information security awareness, and could also assess the compliance to information security policies. An example of a need could be the implementation of a social media policy after several employees accidentally revealed sensitive information using these platforms.

Once a need has been identified, the next phase addresses the development of information security awareness training material, which conveys the required knowledge to the target audience. Typically, the awareness topics would be identified and sources of material would be selected. To continue with the previous example, material could be selected which addresses the potential threats that originate from social media sites and how to mitigate it. In addition, if a policy was created after the incident described earlier, then the application of the policy would be described using the developed material.

It is important to decide if the training material should be developed in-house or procured from external entities. Developing the material in-house could delay the implementation of the information security awareness program as the material must be developed before the awareness program can commence, but it can be more cost effective. On the other hand, procuring the material could accelerate the implementation time but it could cost more.

Another aspect which should be considered is the customisation of the material. Each environment is different and the material should address the specific environment and culture to improve effectiveness. For example, material which is designed for a technical audience would not be effective when presented to a group who are not technically inclined.

The third phase addresses the implementation of the awareness program. The first two phases identified the need and then the selection of a solution. The third phase is the implementation of the selected solution. Individuals have different learning styles and numerous tools are available to deliver the content of the material to the intended audience (Felder & Silverman 1988, Kolb & Kolb 2005). Examples of delivery tools include computer-based training, in-person training, games, dialogues, posters and newsletters. The selection of these tools should be considered with the company constraints in mind, for example, employees might not have time to attend in-person training during work hours, but could do computer-based training outside working hours. Factors which could

also affect the selection of the tool are the learning styles of the group and the group's existing knowledge. For example, some individuals might be introverts; for these individuals, group training and dialogue sessions might not be as effective as using computer-based training or games.

The final phase of the NIST framework is putting mechanisms in place to measure the effectiveness of the implemented program. The use of assessments could provide quantifiable data to measure the effect of the implemented awareness program. Questionnaires and surveys are used in the majority of assessments. However, the use of questionnaires and surveys merely tests the recall of facts (Palmer & Devitt 2007). The use of dialogues could demonstrate understanding and application of the knowledge acquired (Woodford & Bancroft 2006). However, the use of dialogues as part of an assessment requires skilled personnel that have interviewing experience, as well as an understanding of the domain. This could increase the cost of the information security awareness program and delay the progress of the program.

Once the final assessment has been completed, the data may be reviewed to identify possible weaknesses in the information security awareness program, which can be updated accordingly if the program is to be repeated.

Figure 3-8 depicts several mechanisms which would be used under the NIST framework to review and update an awareness program.

The number of threats increases as the technology landscape rapidly evolves. Consequently, the content of an information security awareness program should reflect the threat landscape to ensure that the end user keeps abreast of the threats encountered within cyberspace.



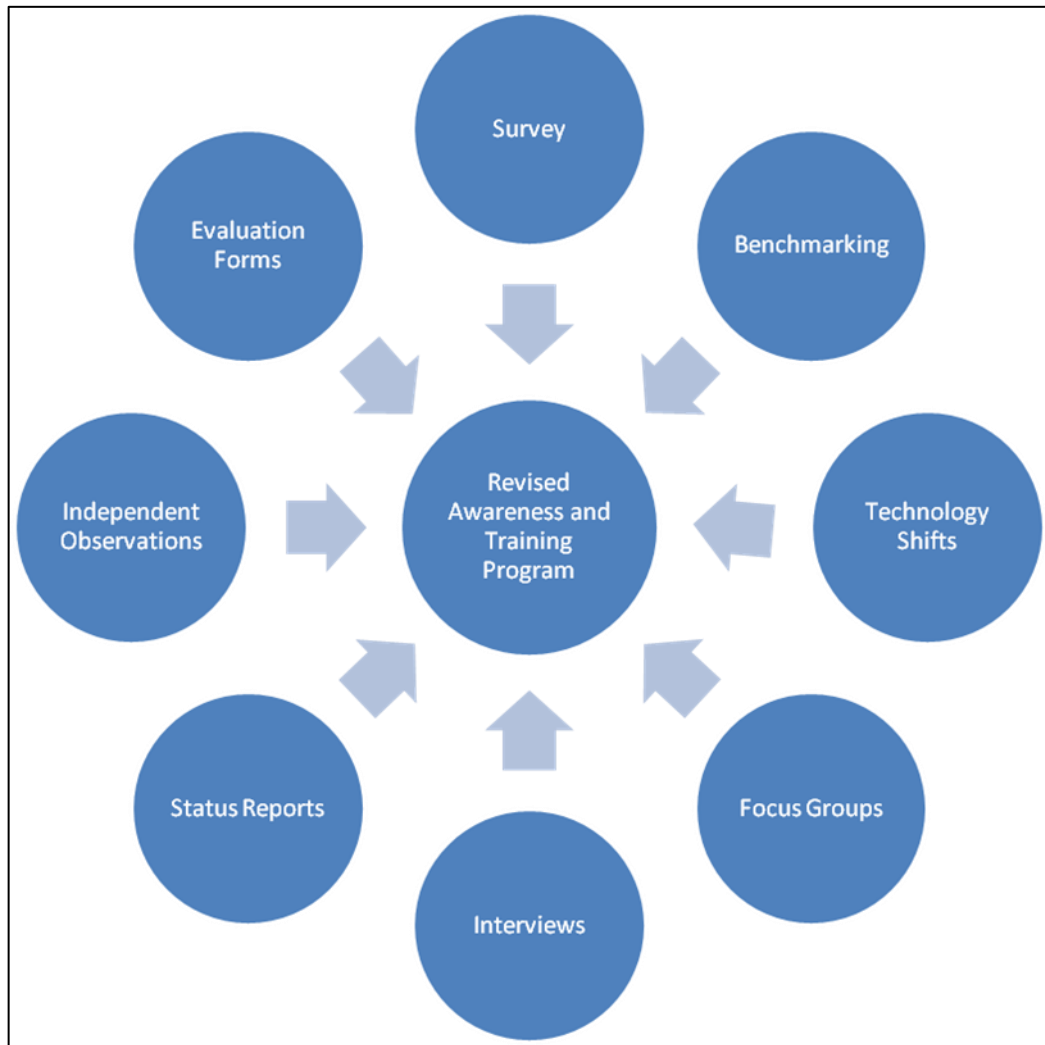


Figure 3-8: Revised Awareness and Training Program Plan (NIST) (2003)

### 3.6.2 Evaluation Result of NIST Information Security Awareness Framework

The NIST framework is ideal for environments which are agile in nature and have a flat management structure. In other words, the NIST framework could be effective in environments that change rapidly and have fewer decision-makers who could delay the program in its entirety. The high-level steps of the framework provide an outline of the milestones, but do not prescribe the details as found within the implementation of the ENISA framework. One of the major advantages of the NIST framework is customisation and time to implement. A potential drawback is the possible misuse of the open design of the framework. Once deployed within a complex environment with several layers of management structures, the NIST framework could pose delays in implementation. These delays could be expected if the detail of each step needs to be formally designed, developed and finally approved by the stakeholders. In addition, resources for each step

also need to materialise, for example the development of a project charter before the program can formally be approved and rolled out.

### 3.7 Selection of Information Security Awareness Framework

The previous sections described the ENISA, SANS and NIST frameworks, which can be used for the design, development and implementation of an information security awareness programs. Each of these frameworks has drawbacks and advantages that should be taken into consideration. The analysis of the environment of the company where the information security awareness program will be deployed is critical to the success of such a program.

Usually due to a lack of funds and time, the selection criteria for the information security awareness framework requires that the framework should be expeditiously designed, developed and implemented. Furthermore, the framework should allow for customising the environment. All environments pose different challenges, and the ability to customise provides latitude to adjust to the environment's needs.

Table 3-3 lists the criteria used for the selection of the information security awareness framework used for this study.

**Table 3-3: Selection Criteria for Frameworks**

	<b>ENISA</b>	<b>SANS</b>	<b>NIST</b>
Implementation Time	Long	Medium	Short
Customisation	No	No	Yes
Additional Resources	No	Yes	No

Funding and availability of participants for the information security awareness program as conducted for this research study contributed to the time limitation to implement the information security awareness program. Students from a residential South African university participated in this study; subsequently it was important that the implementation of the information security awareness program should not negatively impact their schedules. The students were located in another province in South Africa resulting in travel time and expenses for the researcher. Subsequently the completion of the information security awareness program was conducted in a single day. Furthermore, the framework had to be customised to the environment with respect to the time to complete the deployment of the information security awareness program.

The NIST information security awareness framework was selected as it complies with the requirements of this study. Although the NIST framework does not provide additional resources, the concept of metrics was adopted from the SANS framework, as it was deemed a useful addition to the NIST implementation. The use of metrics within an information security awareness program provides the capability to measure effectiveness of the awareness program.

### **3.8 Conclusion**

The need for use and adherence to standards was addressed in this chapter. Standards can facilitate the desired outcome of increased information security awareness. This is a critical metric required by organisations to establish confidence within the business domain.

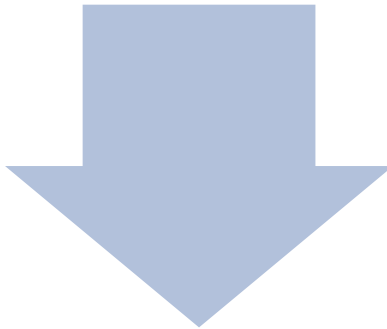
This chapter also addressed the identification of information security awareness frameworks that can be used for the implementation of an information security awareness programs. Three frameworks were analysed to obtain a better understanding of each framework.

Finally, an information security framework was selected which was best suited for the research to be conducted within this study. The NIST framework is simplistic in design and allows for customisation to the environment. The following chapter describes the design and implementation of an information security awareness program, and shows how the NIST framework was used within this study.



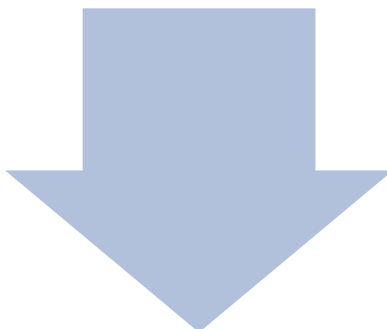
## Chapter 4: Using NIST within an Information Security Awareness Program

Chapter 3 - Information Security Awareness Program



### Chapter 4 - Using NIST within an Information Security Awareness Program

- 4.1 Introduction
- 4.2 NIST Security Framework
- 4.3 Conclusion



Chapter 5 - Design of Information Security Awareness Program

Figure 4-1: Layout of Chapter 4

## 4.1 Introduction

The previous chapter analysed information security awareness frameworks from the European Network and Information Security Agency (ENISA), SysAdmin, Audit, Networking and Security (SANS) and the National Institute of Standards and Technology (NIST). The analysis resulted in the selection of the NIST framework as best suited for this study.

Chapter 4 provides a discussion of the research conducted at each phase of the NIST framework (2003) to implement an information security awareness program targeting the end-user. The main objective of the research was to determine the effectiveness of using games within an information security awareness program.

## 4.2 NIST Security Framework

The NIST security framework was described in detail in Chapter 3. The following sections briefly describe how each of the NIST information security awareness framework phases was applied in this study with the aim to determine the effectiveness of games as a delivery tool within an information security awareness program (See Figure 4-2 depicting detail discussions to follow in subsequent chapters).

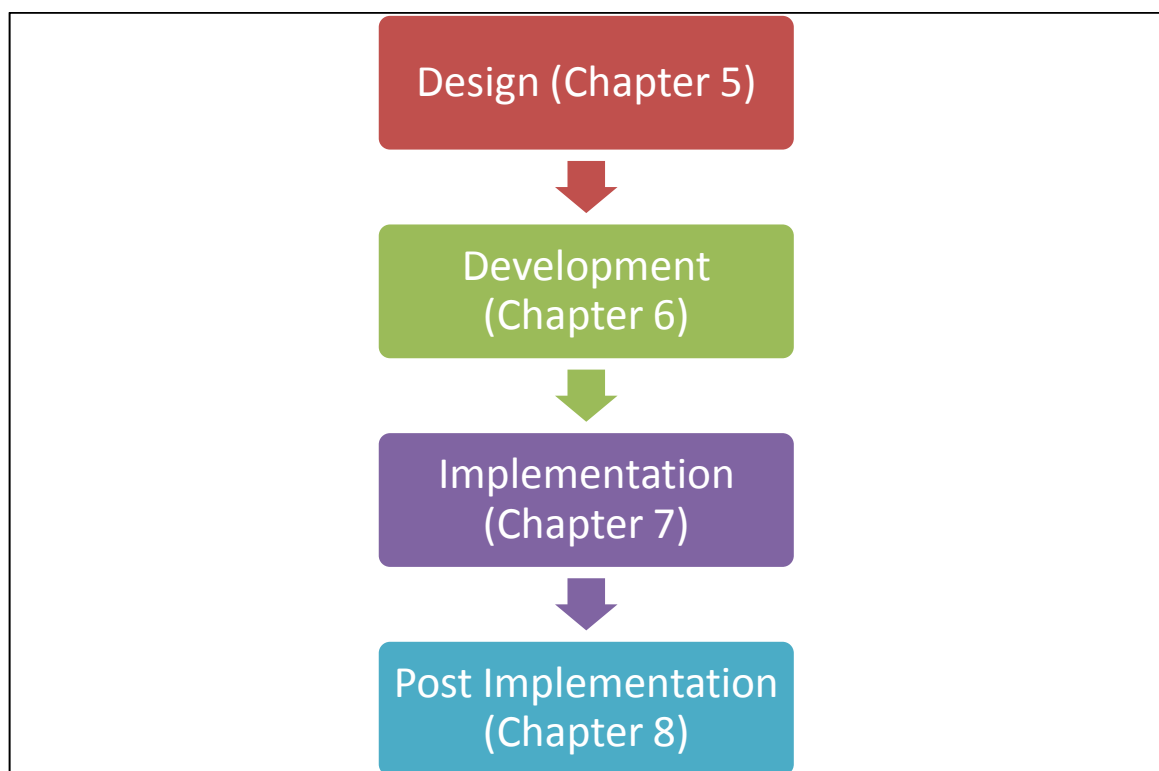


Figure 4-2: Mapping of NIST Phases to Dissertation Chapters (Source: Own)

### **4.2.1 Design**

The initial phase of the NIST framework identifies the need to conduct an information security awareness program. The preliminary study discussed in Chapter 5, conducted with Internet Café users (Section 5.2) as well as social media users (Section 5.3), highlighted the need to develop and implement an information security awareness program to secure these novice computer users. The need to secure the end user is also supported from the discussion in Section 2.3. This is highlighted by the increase in cyberattacks and the ineffectiveness of current technical security controls. These users, who have neither the technical background nor the protection provided by organisations, need the knowledge to mitigate threats originating from cyberspace.

In many cases, employees are protected against threats by the security implemented in their work environment by their organisation, which includes information technology security experts, firewalls, anti-virus software, anti-malware software, operating system updates and information security awareness training (Dutta & McCrohan 2002).

These employees may also have computer systems at home, however, the security measures provided at work does not always apply in the home environment due to lack of funds and/or skills. In some cases, these employees might not have computers at home and they may share computers communally, as in the case of Internet Cafés. These users access resources on the Internet for several reasons, including but not limited to online banking, to purchase items online or make account payments. The use of social networking sites have also been identified as a reason to access the Internet, as these platforms allow friends to stay in touch, make new acquaintances or share ideas.

It is imperative to understand what threats can be encountered by users who access resources on the Internet and develop an information security awareness program to provide these unsuspecting home end-users with the necessary skills to mitigate these threats. Chapter 5 addresses the threats which could be encountered by such users who frequently access resources on the Internet. It also discusses social networking sites in more detail. The threats identified in Chapter 5 confirm the need for an information security awareness program. The tactics that mitigate these threats are also identified. These tactics form the topics of the information security awareness program.

### **4.2.2 Development**

The second phase of the NIST framework addresses the identification of the topics required for the information security awareness program, which stem from the needs analysis described in the previous section. Another requirement for the development phase is the identification of a source for the material to be used during the information security awareness program. It can either be developed or obtained from a third party. A proposed Shared Public Security Awareness (SPSA) system was designed by the author as a vehicle to deliver an information security awareness program by means of a turnkey solution. This system would automatically conduct an information security awareness program once deployed. One of the components of this SPSA system includes gaming as a method to deliver the content of the selected information security awareness content. The design requirements for the SPSA system, as well as the game, are described in Chapter 6. However, the full development and implementation of the SPSA system forms part of future work. The identification of components which increase the knowledge transfer of information security topics is pursued first, and forms part of the completion of the SPSA system.

### **4.2.3 Implementation**

Once the needs have been identified and topics have been selected for the information security awareness program, the next phase of the information security awareness program is the implementation phase. This phase focuses on the different aspects required to deliver the information security awareness knowledge to the intended audience. Chapter 7 describes the implementation phase of the NIST security framework. This includes a discussion of the research design, the methodology used, limitations and ethical considerations. The implementation phase resulted in the data generation, which was used in this study to determine the effectiveness of game play within information security awareness programs.

### **4.2.4 Post Implementation**

The last phase of the NIST security framework requires the evaluation of the implemented information security awareness program to improve the effectiveness of the program. Chapter 8 analyses the data collected during the deployment of the information security awareness program and concludes by discussing the findings, which could potentially be



used to improve an information security awareness program that contains a game or games as a component.

### **4.3 Conclusion**

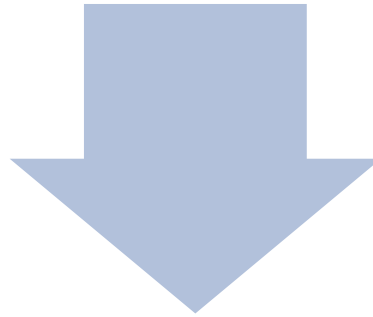
This chapter described the application of the NIST information security awareness framework within this study to determine the effectiveness of games as part of information security awareness programs. An overview of each phase of the NIST security framework is provided and mapped onto the individual chapters which are to follow.

The next chapter addresses the design phase of the NIST information security awareness framework, which focused on the identification of a need and selecting the topics for the information security awareness program.



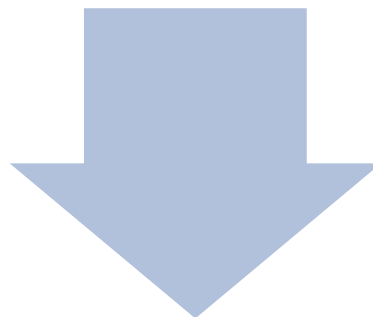
## Chapter 5: Design of Information Security Awareness Program

Chapter 4 - Using NIST within an Information Security Awareness Program



### Chapter 5 - Design of Information Security Awareness Program

- 5.1 Introduction
- 5.2 Needs Assessment from Shared Resources
- 5.3 Needs Assessment from Social Networking Sites
- 5.4 Topics Identified for Information Security Awareness Program
- 5.5 Conclusion



Chapter 6 - Development (Distribution Platform)

Figure 5-1: Layout of Chapter 5

## 5.1 Introduction

The previous chapter provided an overview of the NIST information security awareness framework which was selected for this study.

The first step of the NIST framework focuses on the design aspects of an information security awareness program and hence, the identification of the need for information security awareness training within a selected environment. This chapter describes the needs assessment conducted within an environment, where multiple users utilise shared computer resources to access resources on the Internet, for example an Internet Café.

An experiment was used to identify the threats originating from social networking sites, which highlighted the additional need to develop content to address the threat originating from these platforms. Two case studies were considered for the assessment of information security needs as prescribed by the design phase of the NIST framework (Figure 5-2). Both these assessments are critical for empowering the end-user with knowledge to mitigate the wide variety of threats emanating from cyberspace.

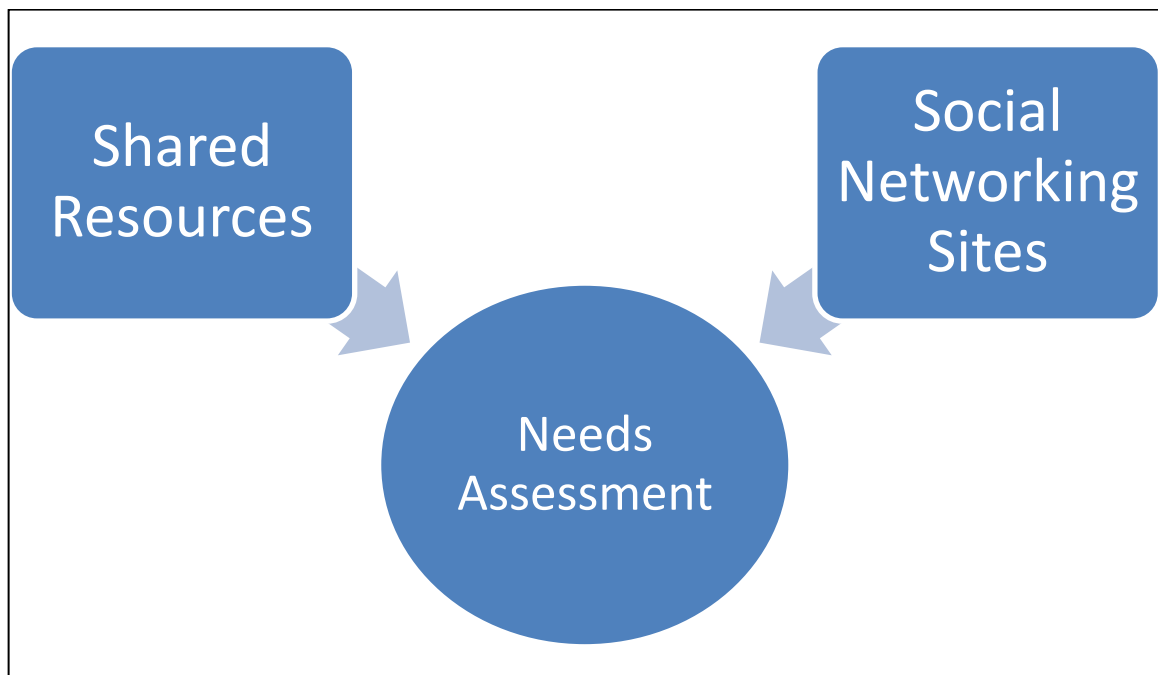


Figure 5-2: Needs Assessment (Source: Own)

## 5.2 Needs Assessment from Shared Resources

Shared resources in the context of this study are defined as multiple users operating different platforms to access resources on the Internet, for example an Internet Café or Virtual Office. In either of these environments, a user would use a platform, for example a

laptop or workstation which is shared between multiple users. The threat exists that other users could have performed actions to directly or indirectly compromise the platform. When a user directly compromises a system, they could deliberately perform nefarious actions: for example, install a keylogger to capture keystrokes entered by the unsuspecting user. An indirect compromise entails a user unknowingly infecting the platform with malware. This can easily be achieved when users visit a malicious website or open an email with embedded malware.

The following sections describe research conducted on Internet Cafés as part of a needs assessment.

### **5.2.1 The Internet Café Industry in South Africa**

An Internet Café is a business which operates by providing individuals with access to services including the Internet, computers and printers. For example, a person can visit an Internet Café to use online banking to pay for goods purchased – saving time and money since they do not have to go physically to the premises of a bank. An Internet Café also provides additional supplementary services, such as printing and editing of documents. These additional services add to the value chain of the Internet Café.

Hyde-Clarke (2006) noted that affluent areas charge higher rates at Internet Cafés than poorer areas. This could be due to the business model, which adapts pricing to customer demographics. In addition, they also noted that the more affluent areas utilise Internet access for business activities, while less affluent areas focused on general use of the Internet (for example, searching for employment). This aligns with the current trend of businesses adopting an online presence to increase visibility to potential customers and also to decrease costs. Hobbs and Bristow (2007) conducted a study on the number of Internet Cafés located in Johannesburg. They found an increase of these establishments in less affluent areas. This could be due to the costs of having computers and Internet access during that period. An Internet Café addressed the need of using a computer and also accessing the Internet without procuring expensive equipment and leasing an Internet connection, which would have been used occasionally. They also found that 65% of the users were repeat users, which implies that access to the Internet was an important part of the users' daily lives, but high costs prevented them from buying a computer and having their own access to the Internet. This study also identified the need for training, including computer literacy training.

In both these studies, the need for Internet access by less fortunate citizens of society has been highlighted. However, these users are only concerned with access to the Internet and might not be aware of the threats lurking within the domain of cyberspace.

Threats are considered as an entity that seeks to breach security, for example cybercriminals. An attack vector is the medium through which the threat is exploited and can thus be considered as a vulnerability or weakness of the system. Attack vectors are relevant as they will be used in the development of information security awareness material, where the nature of each vector will be explained to the user. Therefore, it is essential to consider both the threats and the attack vector. Core to the needs assessment and the completion of attack vectors, is a literature study to identify threats and Internet uses.

The next section addresses the Internet uses which could subsequently assist in identifying the associated threats.

### **5.2.2 Internet Uses and Threats Mapping**

The Internet can be used for a wide variety of applications, including but not limited to email, social networking, information searches, banking and shopping. Furuholt, Kristiansen and Wahid (2008) discuss the various uses of the Internet which include chatting, doing business, taking online courses and various administrative activities. These uses are classified under different high-level categories, which allow the author to include other uses in future. Accessing social networking sites are added to the uses of the Internet as identified by Furuholt et al. (2008). Social media sites which include social networking sites have been widely adopted by users and have been integrated into society. The listing of the uses and the categories are depicted in Table 5-1. The listing provides a classification of attack vectors into categories.

Next the threats associated with each category are discussed. Duality within Internet use also exists, as cybercriminals have developed tactics to prey on unsuspecting users and subsequently are using the Internet for nefarious purposes. A literature study on Internet threats was undertaken in order to determine possible threats. Research done by Anselmi and Boscovich (2010); Menon and Gabrielv (2010); Kim et al. (2011); Evans (2010) and Manning (2010) are considered collectively with the following threats identified: worms, Trojans, password/info stealers, adware, backdoors, viruses, exploits, spyware, phishing, downloaders, droppers, ransomware, social engineering and rootkits.

**Table 5-1: Classification of Internet Uses**

<b>Types of Internet Use</b>	<b>Category</b>
Downloading software for professional use	Business
Doing business such as freelancing	Business
Email	Communications
Social networking	Communications
Chatting	Entertainment
Playing Computer games	Entertainment
Downloading software for amusement	Entertainment
Downloading music	Entertainment
Visiting pornographic sites	Entertainment
Gambling	Financial
E-shopping	Financial
Internet Banking	Financial
Seeking information	Information
Reading online news	Information
Doing Research	Information

Menon, Gabrielv (2010) and Evans (2011) also discuss threats such as browser-based attacks and attacks through social media. Browser-based attacks can originate from vulnerabilities in, for example, Firefox (FF), Internet Explorer (IE), Portable Document Format (PDF), Shockwave Format (SWF), ActiveX and Microsoft (MS) Office, amongst other software. Moreover, when considering research from F-Secure (2008), the following threats emerged: identity theft, spam, hacking, denial-of-service, violation of digital property rights and cyberbullying.

The results from the literature study described various threats that are associated with Internet use and even more strongly associated with Internet Cafés. This clearly indicates the need for an information security awareness program to protect Internet users against these threats. Due to the perceived technical difficulty of using computers, the end-user (who usually only cares about using the Internet) may not be concerned about security concepts (Padayachee 2012). It is therefore critical to address the lack of information security knowledge with an effective information security awareness program. This requires the adoption of new precautionary behaviours to protect the end users from threats.

The mapping of threats and uses as part of the needs assessment process is discussed next. The analysis of the mapping between the Internet uses and the threats would result

in the identification of information security awareness topics applicable to Internet Café users, and also to end-users in general.

Table 5-2 maps the Internet uses in the columns against the threats identified in the rows. Certain threats are grouped together to provide a high-level category. For example, malware is a high level category that includes viruses, spyware, Trojans, keyloggers, worms and the like.

Ticks, denoted by the symbol '✓', are used to indicate which threats can be associated with a particular use. The symbol 'X' denotes "not applicable". An example is that physical harm cannot occur while searching for information on the Internet. The tick symbol denotes that the threat is applicable to the given use. An example of a threat applicable to a given use is a web browser that can be exploited via vulnerabilities when using it for entertainment purposes. A user might want to watch a movie online with the use of a web browser. However, the movie could be hosted by cybercriminals who have deployed malicious scripts to exploit vulnerabilities within the web browser.

The symbol 'P' denotes "partial applicability". This is used to indicate that the threat can apply only in certain circumstances. An example is a phishing attack where a user's information can be harvested through an information search, for example in reports. Some websites require the user to provide personal details to obtain access to the content. The user cannot verify that the website would adhere to a policy regarding the sharing of captured data with external entities.

### **5.2.3 Selection of Topics**

The previous section mapped Internet uses against the different threats which could be encountered. It is therefore important to identify and prioritise the threats end-users face when using shared resources, especially within Internet Cafés. A discussion of the relevance of the threats is discussed next.



**Table 5-2: Mapping of Internet Uses to Threats**

<b>Threat \ Use</b>	<b>Info</b>	<b>Entertainment</b>	<b>Financial</b>	<b>Business</b>	<b>Communications</b>
Spam	✓	✓	✓	✓	✓
DoS	✓	✓	✓	✓	✓
Phishing	P	P	✓	✓	✓
Violation of digital property rights	✓	✓	X	✓	P
<i>Malware</i>					
Virus	✓	✓	✓	✓	✓
Adware	✓	✓	✓	✓	✓
Scareware	✓	✓	✓	✓	✓
Spyware	✓	✓	✓	✓	✓
Worms	✓	✓	✓	✓	✓
Trojans	✓	✓	✓	✓	✓
Password/Info stealer	✓	✓	✓	✓	✓
Backdoor	✓	✓	✓	✓	✓
Downloader	✓	✓	✓	✓	✓
Dropper	✓	✓	✓	✓	✓
Rootkit	✓	✓	✓	✓	✓
<i>Browser Based</i>					
Firefox	✓	✓	✓	✓	✓
IE	✓	✓	✓	✓	✓
PDF	✓	✓	✓	✓	✓
SWF	✓	✓	✓	✓	✓
ActiveX	✓	✓	✓	✓	✓
Opera	✓	✓	✓	✓	✓
MS Office	✓	✓	✓	✓	✓
<i>Hacking(Exploit)</i>					
Social engineering	X	✓	✓	✓	✓
Inherent software vulnerabilities	✓	✓	✓	✓	✓
Patch management	✓	✓	✓	✓	✓
Online scams and fraud	✓	P	✓	✓	✓
Physical harm	X	✓	X	X	✓
Cyberbullying	X	✓	X	X	✓
Spreading false or negative information	X	✓	X	X	✓
Illegal online gambling	X	X	✓	✓	P
Identity Theft	X	P	✓	P	✓

It is important to take into consideration what the end-user has control over when using shared resources as in the case of Internet Cafés. The threats identified in Table 5-2 are analysed with regards to locus of control. In addition, the threats which the user have control over have been highlighted. This creates a segregation of responsibilities and delineates what security topics should be covered in the information security awareness program. In the case of spam, the end user has no control as the email provider should

have mechanisms in place to prevent spam from reaching the user's email box. The end-user usually does not have the required skillset to configure spam filters on his or her email box. Service providers should implement measures at a higher level to prevent spam from reaching the end-user's email box. That been said, the end-user could tag an email as spam to prevent future spam from the same source (Google Inc 2014).

DoS attacks are also technically advanced and the end-user would not have the skillset to mitigate such an attack (Mirkovic & Reiher 2004). The prevention of a DoS attack is delegated to the Internet Service Provider (ISP). Such an attack focuses on the targeting of the resources and ultimately drains the target from any processing power, resulting in no service (Cricket 2013). The violation of digital property rights also falls outside of the realm of the Internet Café end user and will not be discussed further. In other words, the establishment in this case, namely the Internet Café, could have facilities to reproduce digital content, which is illegal. The end-user has no control over what facilities such establishments use as part of their business.

Malware could in the majority of cases be mitigated by anti-malware tools which include anti-virus (AV) software. The end-user would ultimately not be aware of malware when effective anti-malware tools are deployed with the exception of zero-day exploits. The threat of malware is transferred away from the end-user to the establishment providing Internet access.

Web browsers are commonly used to access content on the Internet. Many of the threats originating from the Internet entice the users to perform actions which under normal circumstances they would not have considered. In the case of shared resources, the threat management of malware should be implemented and managed by the establishment. This extends to all software installed on the shared resources, including the Office suite (Word, PowerPoint and Excel), Java and Acrobat Reader. Many web browsers utilise third party software to extend their capabilities but these also inherit the same threats that effects software. The establishment should ensure these are also protected against attacks and possible exploitation: usually this protection could be achieved through patch management.

The remaining threats – phishing, social engineering, scams, cyberbullying, physical harm, spreading of false or negative information, illegal online gambling, and identify theft – are all considered relevant threat topics for end-users who visit establishments where

resources are shared. Social networking is added to the list, as many new threats have been created to use it as a platform to target unsuspecting users (Sadeghian, Zamani, & Shanmugam, 2013).

These threats, which the end-user can control, are summarised into high level topical categories and are depicted in Figure 5-3.



**Figure 5-3: Threat Vectors for Internet Café (Source: Own)**

It should be noted that the end-user can have control over the threats identified in Figure 5-3. In other words, the threat has a low enough technical level allowing the end-user to make an informed decision on what measures to implement to mitigate the threat. For example, in the case of a phishing attack, the user can choose not to click on the link and also not to provide information requested from the phishing site. The other threats, excluded from Figure 5-3, may include a technical component which a non-technical user would not be able to mitigate. For example, a DoS attack is whereby attackers deploy attacks against a target platform with the intention to drain the target’s processing ability and ultimately cause the cessation of the platform (Schuba, Krsul, Kuhn, Spafford, Sundaram & Zamboni 1997). The end-user would not have the skillset or the resources to mitigate a DoS threat.

This section has identified the needs of establishments which use shared resources to allow multiple end-users to access the Internet. The literature study regarding Internet

Cafés was used as the design phase of the NIST security framework, to identify the need and subsequently identify potential information security awareness topics. The following section addresses the threats encountered on social networking sites. The results from the experiment conducted are then combined to identify a recommended list of information security awareness topics.

### **5.3 Needs Assessment from Social Networking Sites**

The previous section determined the different threat vectors that cybercriminals use to target unsuspecting users. This section addresses one of the identified threat vectors, namely social networking sites. This section also investigates, with the use of an experiment, the information security awareness knowledge of users on these sites. Social networking sites have been widely adopted by users for several reasons, including business and personal use.

The first phase of the information security awareness framework is to conduct a needs analysis as part of the design. This section forms part of this first phase of NIST by using an experiment to demonstrate the ignorance of users on social networking sites, as well as to determine how data on these platforms could be used for nefarious purposes.

Section 5.3.1 provides an overview on the use of the digital environment to profile users who frequent Internet sites. These techniques include linguistic analysis and personality profiling using data located in the public domain. Section 5.3.2 discusses the experiment used to collect and analyse the data from the public domain. Section 5.3.3 provides an explanation as to how the analysed data could be used to target users on social networking sites. The section concludes in Section 5.4 with the identification of topics to address the social networking threats.

#### **5.3.1 Related Research**

This section describes how attacks within the digital environment could be crafted by cybercriminals. Social engineering attacks require data to be effective. Social networking sites provide a platform to effectively harvest and collect data. These platforms are designed to allow users to disclose personal information and the business models of these platforms require user data to be publically available (Enders, Hungenberg, Denker & Mauch 2008). For example, advertising companies use this data to target a certain demographic group for certain products. With the advances in technology, websites allow

users to create content. This content could express opinions on topics, as in the case of news websites. Users are not only allowed to express points of view on published articles with the use of posts, but also comment on other user's posts.

These posts and comments could potentially be linguistically analysed to identify social relationships, emotions and thinking styles. Software tools like Linguistic Inquiry and Word Count (LIWC) (Pennebaker, Booth & Francis 2007) could be used for personality profiling from textual data representing human communication (e.g., posts and comments). LIWC is a probabilistic text analysis program that counts words and categorise them in meaningful psychological categories. These categories include but are not limited to positive emotions, negative emotions, social words, anger, etc. (Pennebaker & King 1999). This implies that textual data collected from textual communications could be analysed to profile a target. In the case of the news articles, a user might be negative towards a topic, which in turn may be used by a social engineer to establish trust or as an emotional trigger. LIWC has been used in numerous studies, covering a wide range of topics which included:

- Predicting deception from textual words (Newman, Pennebaker, Berry & Richards 2003).
- Identifying gender differences in language use (Newman, Groom, Handelman & Pennebaker 2008).
- The use of language to identify personality styles (Pennebaker & King 1999).
- Revealing the psychological changes in response in society to an attack as in the case of the 9 September 2001 terrorist attack on the World Trade Center (Cohn, Mehl & Pennebaker 2004).

Other work on the effect of personal disclosure on social networking site includes:

- Evans, Gosling and Carroll (2008) concluded that men are more likely to disclose political views than women. Their work focused on the possibility of revealing one's personality through social networking sites.
- The use of function words within sentences offers insight into the honesty, stability, and sense of self of the person (Fiedler 2007).

- The use of language in self-narratives could be used to determine personality types (Hirsh & Peterson 2009).
- An investigation by Ryan and Xenos (2011) summarised the 'Big Five' and the usage of Facebook. The Big Five are defined as five broad domains or traits of personality that are used to describe human personality: openness, conscientiousness, extraversion, agreeableness, and neuroticism. For example, neurotic people are easily stressed and upset (Vollrath & Torgersen 2000). These traits can easily be exploited by social engineers.
- The Department of Homeland Security from the United States of America investigated the possibility of predicting when terrorists might launch an attack (Vergano 2011). The predictions were deduced from 320 translations of Arabic documents released by the terror groups: al-Qaeda, al Qa'ida, Hizbut-Tahrir, and the Movement for Islamic Reform in Arabia (MIRA).

The use of social networking for nefarious purposes also extends to terrorists groups who have used this medium as part of their operations, including information gathering and recruitment of potential members. The following work has been conducted on the use of social networking sites and terrorists:

- At the University of Arizona Dark Web Terrorism Research Centre, complex models have been built to study extremist-group web forums and thus construct social network maps and organisation structures (Chen 2012).
- Ressler (2006) highlighted the importance of understanding the recruitment strategies employed by terrorist organisations and this further extends to comprehending the reasons why members of society would join such an organisation. The use of social network analysis could prove useful in countering such recruitment strategies.
- The various techniques used by terrorist organisations are addressed by Veerasamy and Grobler (2011). Recruitment of new members to the terrorist organisation was critical for the survival of the organisation. The new recruits were identified by their psychological characteristics revealed through their expressive writing.

This is not an exhaustive list of the work conducted in the field of terrorism, but it clearly demonstrates how extremist groups are using social networking platforms for their operations. It also highlights that social media sites, which includes social networking sites, have information which could be abused if it lands in the wrong hands. The next section discusses an experiment conducted to demonstrate how social media users disclose information which could be employed with detrimental effect.

### **5.3.2 Social Media Profiling Experiment**

The following sections describes the experiment that collected publicly available data from an online news site, and describes how this data could be used to conduct a social engineering attack. The findings from the experiment demonstrated that the majority of users on Facebook do not apply security control correctly resulting in the leaking of personal data.

#### **5.3.2.1 Disclaimer**

This experiment only collected data to demonstrate the ease of harvesting data from the public domain. Typically, the collection of data is the first phase of a social engineering attack. With regards to users of Facebook, the only action was that of making a friendship request to a user. It should be noted that one of the features of Facebook is the capability which allows users to send friendship requests to other users (Sieber 2013). In the context of this experiment, the intention was to determine how many of the users would accept a friendship request from an unknown user. If the user who was originally sent a friendship request, accepts the friendship request, then this was noted by the author. The user was “unfriended” after the experiment. A legitimate Facebook account was used during the experiment, as the use of fake personas violates the terms of use of Facebook. Data analysis was used to determine potential victims based on emotional response to content; no mechanisms were used to test the findings. No automated tools were used during the data collection, as this also violates the terms of use of most social networking sites, including Facebook.

#### **5.3.2.2 Experiment**

Social engineering consists of the following phases: the collection of target data, data analysis to understand what vulnerabilities exist, and finally exploiting the identified vulnerabilities (Barrett 2003). The attack is applicable to the digital and physical world. For example, within the digital world, scanning a network forms part of the data collection

phase; followed by data analysis to identify potential targets; finally, an attack is launched against the targets with identified weaknesses.

In the physical world, people dispose of papers containing data, such as statements from credit cards, banks, and other accounts. This could provide information about the financial status of the person. Subsequently, a social engineering attack could be personalised using the collected data. The two worlds, physical and digital, are starting to overlap with the advances in technology, with the results that data collected in one world can be used in the other.

The design of this experiment involved the manual collection of data from a social media news site. The articles with the most responses were considered for the experiment. Users are allowed to respond to the article with a post and respond to other posts from other users with a comment. Users who create responses are required to login using Facebook account credentials or an account created on the site. A user who creates a response indirectly discloses the following data:

- Username – A pseudonym is used for identity purposes.
- Textual data – The response which expresses the opinion of the user.
- URL to Profile – The URL to the profile on Facebook is embedded in the link used to display the username.

This information does not have value to the general public. However, in the hands of a seasoned cybercriminal, this could have a significant impact, especially in the case of social engineering.

In this experiment, the responses, together with the URL, to the profile were manually captured. No personal information was collected except for the URL. This data was utilised to determine the following:

- What data could be collected using the profile?
- What information can be deduced from the responses created by the users?

The answers to these questions are discussed next:

- **Using Profile** – A list of unique profile URLs were manually generated from the response data collected. Each of these URLs was visited to determine how much data is disclosed in the public domain. In other words, the Facebook account was



visited, using the URL, without logging into the social networking site. This is important as users who do not know how to configure controls, do not know how to limit the amount of data exposed to the public. A summary of data disclosed includes the following:

- Activities and interests
- Friends Listing
- Contact information

Next, the URLs were visited once more. However, in this case the profile was visited from an authenticated account – in other words, logged in to a Facebook account. The same data was noted and compared against the data from the non-authenticated session. The same web browser was used for the data collection.

The next phase of the experiment was sending a friendship request to the profile. The status of the friend request was also recorded. The status conditions are defined as requested, accepted, not enabled or message (As depicted in Table 5-3). There are no responses sent to the requestor if the friendship request is declined. Hence, no state is created to indicate declined friendship requests.

**Table 5-3: Status description**

State	Description
Requested	A friend request has been sent and is pending
Accepted	The friend request has been accepted
Not Enabled	Friend request feature disabled by user
Message	Friend request was not accepted but message was sent from user

The friend requests are used to determine the susceptibility of users to accepting a friend request without verifying the trustworthiness or some identity of the user who sent the request.

This section described the collection of data from profiles where users had failed to apply the necessary security controls to limit the exposure of sensitive personal information. The next section discusses the threat vector that textual data could present to social media users.

- **Using Responses Created by Users** – The responses were harvested during the collection of the data from the social media site. These responses represented

posts and comments expressing points of views. Only the textual data of the response data was stored in a database. This data included the profile name as posted on the news website, URL linking to the Facebook profile and the message posted.

The intention of the experiment was to demonstrate that responses could be linguistically analysed to determine emotion. Using the description of the article and the analysed emotion, a deduction can be made indicating a user's sentiment regarding a topic. The stored data is programmatically extracted and analysed using the LIWC software. Subsequently, the different responses are mapped against the different emotional dimensions, which include anger, positivism, negativism, etc.

The result set is also stored within the database for further analysis. All of these could be used to determine personality traits. For example, work conducted by Pennebaker (2011) has shown that, compared to female users, male users use more articles ("a", "the"), nouns, prepositions, numbers, words per sentence and also swear more. Brodie (2011) showed that the use of certain words could provoke anger in a person, which subsequently would prevent the user from making logical decisions. Thus, a social engineer could have a greater impact when conducting a social engineering attack, which evokes negative emotions or anger. This experiment focused on the identification of negative emotions and anger from the collected responses. This consequently could identify users who are prone to anger or negative emotions, and also identify which topics evoke those emotions.

### 5.3.2.3 Findings

The following section describes the results from the experiment:

- **Data collection** – A total of 353 unique profiles were catalogued from the data set. It also consisted of 791 comments and 728 posts from nine articles published on a social media news website. A friendship request was sent to each social networking user after completing the observation on personal data leakage. It should be noted that no additional interactions were made to the social networking users. A total of 130 requests were sent to users over a period of three days.

However, Facebook issued a warning, which could be attributed to users possibly reporting the receipt of friendship requests as suspicious behaviour. Another reason

could be the security measures from Facebook noted that multiple friendship requests were made from the same Facebook account in such a short time period. Consequently, the author ceased the friendship requests action.

- **Using profile information** – This section discusses the results from the experiment regarding the use of the URL associated with the profile. In other words, what data was disclosed to users who are not associated with the identified profile and an examination of the friendship request responses.

The result from the analysis of the collected data on the disclosure of personal information is depicted in Figure 5-4. Disconcertingly, 59% of profiles visited within this experiment expose data about interests and activities from the profile without the need to log into Facebook. A 20% increase in data leakage is observed once the same profile is accessed from an authenticated Facebook account. It should be noted that the visiting profile is not linked to the profile. In other words, the visiting profile is not a friend of the profile under observation.

Equally important is the availability of the user’s friends listing, which indicates an increase of about 70% visibility using a logged-in Facebook session. The availability of contact information does indicate a slight increase when accessed through a logged in account.

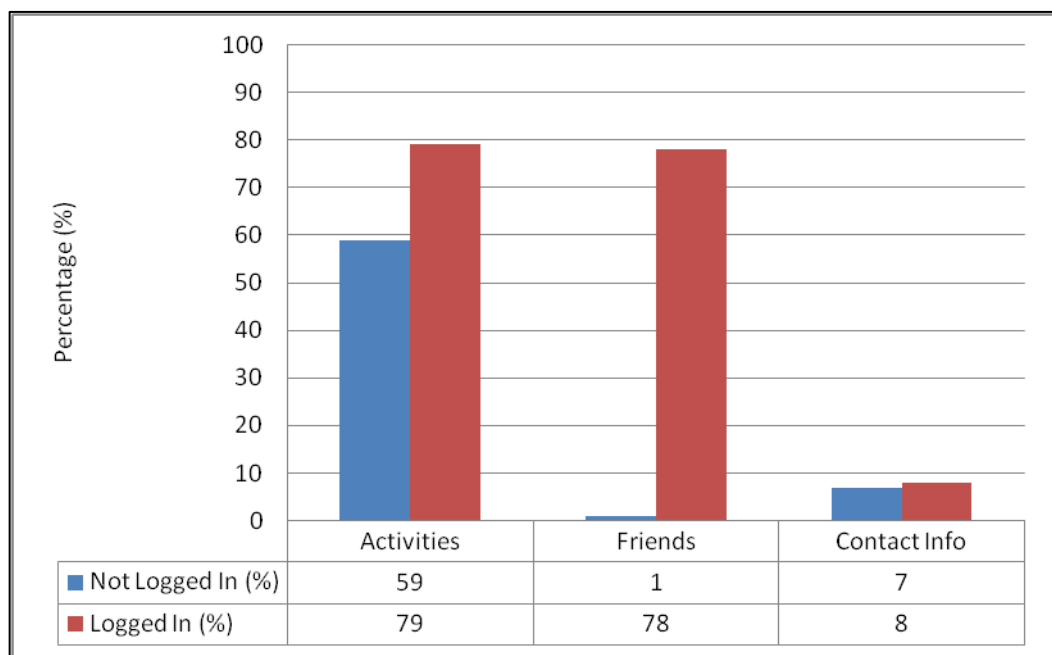


Figure 5-4: Data Disclosure (Source: Own)

Next the results from the friendship requests (Figure 5-5) are discussed. A 35% success rate of accepted friendship requests was obtained from the 130 friend requests sent to the users. Only 4% of users did not enable the “*Send Friend Request*” feature, thus preventing other users from requesting a friendship. An interesting observation is that none of the users who accepted friendship requests sent messages to request additional information from the unknown user to establish trustworthiness.

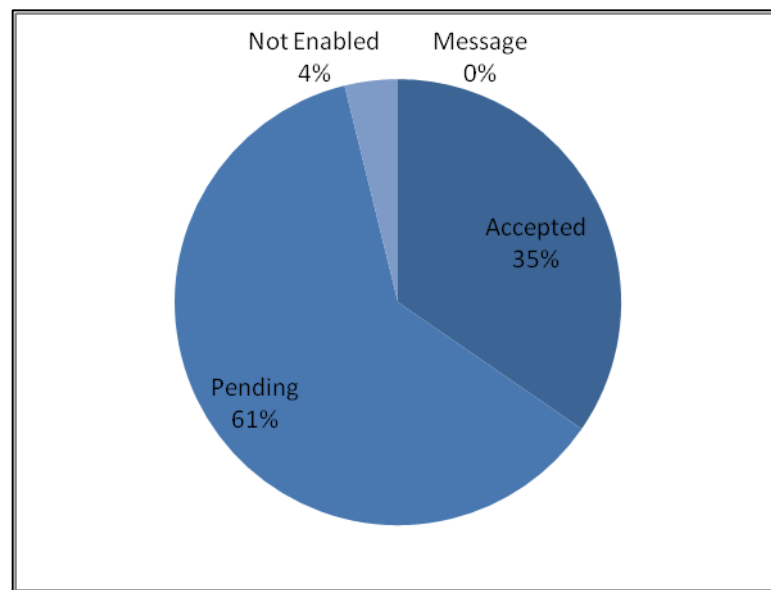


Figure 5-5: Results from Friendship Requests (Source: Own)

- **Using Responses Created by Users** – This section concentrates on the probability to create an attack using the data leaked through the created responses by the social networking user. In other words, the author explores whether exposed data could profile the user through a social engineering attack using emotions.

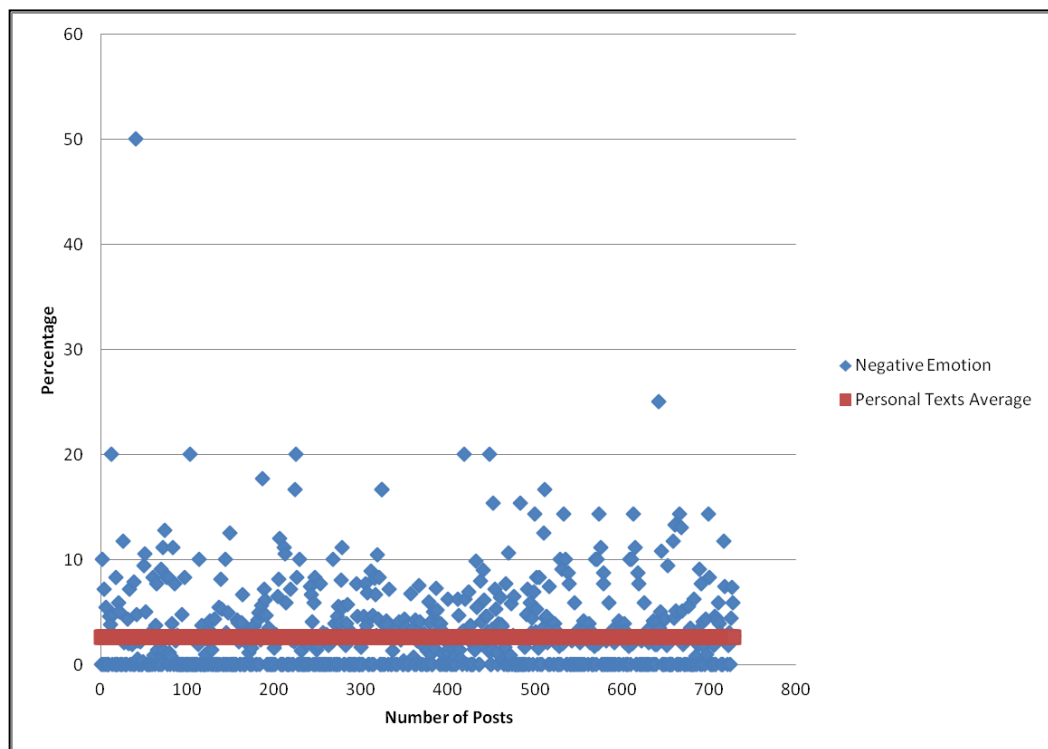
A form of content-specific writing style analysis was performed on the responses. All the posts and comments were analysed to determine the overall average negativity. The negative average of posts was calculated as 2.9% while comments were calculated as 3.03%. As defined earlier, posts are responses to the article, while comments are created in response to what other users have communicated.

The increase in negativity could be attributed to users responding more emotionally to other users when they are biased towards a point of view (Pelled, Eisenhardt & Xin 1999). The mean for personal text, written to express an opinion, is 2.6%

(Pennebaker, Chung, Ireland, Gonzales & Booth 2007). This indicates the existence of posts and comments which are higher than the norm.

Figure 5-6 provides a graphical representation of the analysed posts (indicated by the blue diamonds) with the mean (red line) included. One outlier was observed and removed from the result set. The data represented by the outlier was inspected and it was found that the response contained two words.

From the graphical result set, numerous responses are higher than the mean which implies a higher emotion was evoked. This is essential to a social engineer, who can now select responses with a high negative percentage and link it to a response. Although the data collected did not link the response to a social networking user, a cybercriminal could have collected this data, subsequently identify which users were emotionally triggered by what topic.



**Figure 5-6: Negative Emotions from Posts Analysis (Source: Own)**

In addition, the anger dimension was analysed. This dimension specifically focuses on the use of anger words within textual data for example: furious, angry, mad, offended, disgusted, etc. The analysis parameters were set to only include posts with a higher percentage than 10%, thus producing a smaller victim pool (Figure 5-7).

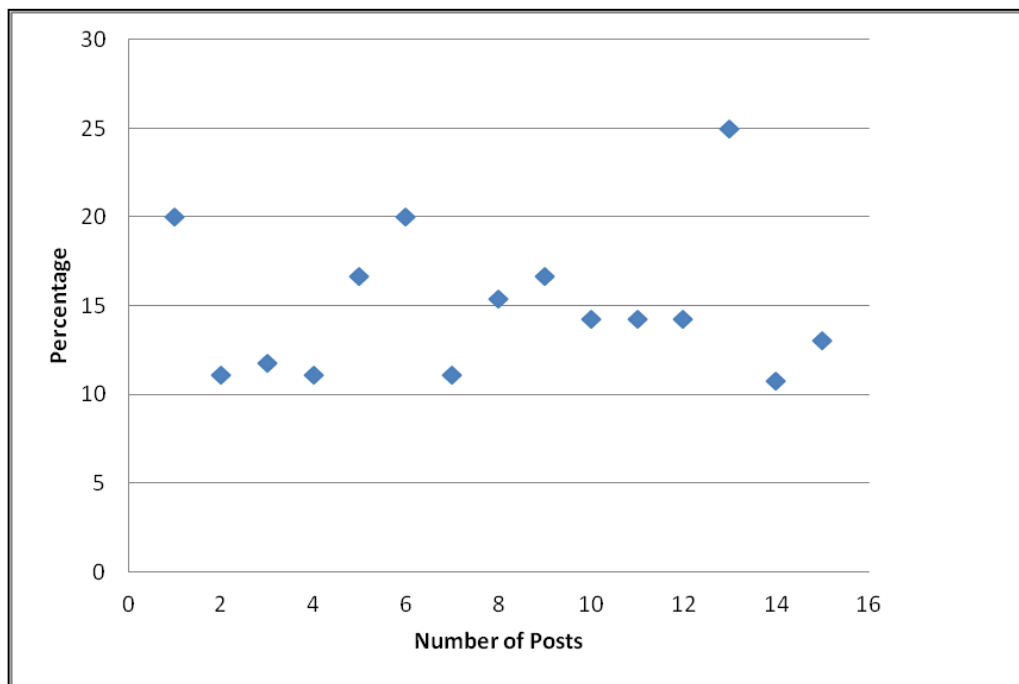


Figure 5-7: Anger Emotions above 10% (Source: Own)

#### 5.3.2.4 Discussion of the Experiment

This section discusses how the information deducted from the data collected in the experiment could be used for nefarious purposes. A wide variety of potential attacks are available to attackers. However, this section focused on using textual data collected from social media in a social engineering attack.

- **Using profile information** – Based on the results from the experiment on the data exposed from profiles, many users on this platform do not apply the necessary tools provided by these sites to control the disclosure of their personal information. This finding is supported by Whitlock (2011), who concluded only 18% of users implement privacy setting controls. It should be noted Facebook updates their privacy controls regularly and users would need to stay updated with the changes implemented. This implies that attackers could easily harvest personal data about users without the need to bypass security measures implemented by social networks.

This experiment found an increase in the availability of data when accessing a profile once logged into Facebook. Also, most users expose their friend lists, which could be used as part of an evil twin attack. An evil twin attack is defined as the use of a rogue profile to impersonate a legitimate profile (Timm 2010). In other words, an attacker could clone a profile by collecting all the required data from another

profile. Once completed the attacker could send a friendship request. The victim could implicitly trust the source based on the familiarity of the requestor information provided with the request, which includes the picture and name of a trusted friend. Another concern is the friend request acceptance rate. The study showed users accept 30% of friend requests without requesting additional information.

- **Using Responses Created by Users** – Content creation by users has been widely adopted by the Internet community, which also provides the society with the right to freedom of speech. For example, users could express their opinion on current news events. However, these users could be profiled and personal traits exposed due to the creation of textual responses which could be programmatically analysed. Profiling takes two approaches: prospective and retrospective (Nykodym, Taylor & Vilela 2005):
  - Prospective profiling involves the development of a new template from previously data collected subsequently using the newly developed template on recently collected data to identify individuals whom resemble the characteristics defined within the created template.
  - Retrospective profiling uses data left behind by users, such as the web browsing history to develop a description of the user.

Retrospective profiling was used during this experiment, since user-created data was used. The use of profiling to identify potential targets could also be used by cybercriminals, especially social engineers.

The results from this experiment demonstrated how easy it was to collect data from the public domain and programmatically analyse textual data to profile potential targets. In addition, attacks could be customised to each target. This is achieved by understanding which topic evokes an emotion or induces a state in the user whereby logical decision making is impaired. The use of this information in a possible social engineering attack is described in the next section.

### **5.3.3 Application of Data Collected to Conduct a Social Engineering Attack**

Cybercriminals could use social media sites, for example online news sites, to collect data about users and subsequently use it in an attack. In the case of online news websites,

users have the capability to create responses to news articles. Attackers could use these responses to craft an attack targeting social media users.

As described in previous sections regarding the use of linguistic analysis, an attacker can identify which topics a user reacts negatively towards. The selection of articles could be attributed to the number of responses generated towards a news article. Next, an attacker could also possibly identify the friends of a particular user. The friends list maybe visible to the public domain due to the incorrect configuration of privacy controls. The experiment has shown that the majority of Facebook users have indirectly exposed their list of friends by incorrect use of the privacy controls.

An attack can be created using the emotion towards a topic and information about a friend from the potential victim. The victim is the target of the attacker. The attacker can create a fake profile on the social networking site using the information collected about the friend. Next, the attacker could then send a friendship request and manipulate the victim to accept the request.

Once the friendship is established, the attacker can continue by creating a malicious file and customising the theme of the file. The theme is aligned with the topic identified which evoked an emotion. Using these two vectors; emotion and friendship, the success of the attack increases significantly. The victim will receive the message with a malicious file (for example a PDF document) from the fake profile, which is the same profile as a trusted friend. The victim could implicitly trust the source and then, due to the emotional trigger used in the message itself, be influenced to open the malicious PDF and infect the computer systems with malware.

#### **5.4 Topics Identified for an Information Security Awareness Program**

The previous section identified potential threats originating from social networking sites, which also confirmed the need to address the topic of social networking as part of an information security awareness program. Subsequently, Sections 5.2 and 5.3 focused on the threats originating from shared resources as seen in Internet Cafés and social networking sites. This resulted in the identification of a need of an information security awareness program targeting novice computer users.

Another outcome from the work conducted is the identification of topics that address the needs of end-users. It should be noted that a wide variety of topics exists within the realm



of cybersecurity. For example, computer security topics include but are not limited to the following: social engineering, denial of service attack, cross site scripting, session hijacking, password cracking, malware, identity theft, scams, phishing attacks, physical attacks, cookie hijacking, hoaxes, spam, network scanning, Intrusion Detection Systems (IDS), Intrusion Prevention System (IPS), security policies, incident response, laptop security, access controls, encryption and decryption, mobile security, evil twin attacks, pharming and browser hijacking. Not all these topics are applicable to the traditional end-user, who does not have an Information Technology (IT) background. The selection of the information security awareness topics applicable to the end-user that frequent the Internet are discussed next.

A web browser is the software tool used by the conventional end-user to access the Internet (Judson 1996). The mere use of the web browser would expose the end-user to threats originating from email, social networking sites and web site. Cybercriminals have several attacks they could conduct from email, social networking sites and website. Section 5.2 identified threats which could triggered when using a web browser. These threats include but are not limited to the following: phishing, social engineering, scams, cyberbullying, physical harm, spreading false or negative information, illegal online gambling and identify theft. Social networking was identified as a threat in Section 5.3.

All these threats are considered in the identification of a list of topics to be included in a security awareness program. An attack tree is used to develop a comprehensive overview of the threats targeting Internet users. Schneier (1999) described an attack tree as a way of thinking to describe the security of a system. It represents the attacks as a tree structure, where the root node is the focus of the attack and the leaf nodes are the attacks which could be performed to achieve the final goal of successfully exploiting the root node.

The first node to consider is the computer used by the end-user. The computer consists of hardware and software components. The physical security of the computer hardware is not considered for this study. The computer hardware cannot be directly affected from an attack originating from the Internet and the measures required to secure the physical components against attacks originating from the Internet are too advanced for novice users. These include but are not limited to removing malware from the basic input/output system (BIOS) and load balancing of the computer processor in the event of a denial of service attack. The software consists of the operating system and other software. The

operating system can be protected against potential threats by downloading and installing updates, while the rest of the system is protected with the use of anti-malware tools which include antivirus (AV) software.

Threats originating from a network are mitigated with the use of a firewall. However, in Chapter 2 it was shown that these measures are not always effective. The end-user uses the web browser as a gateway to the Internet. The web browser is added to the attack tree as this is the next threat vector that could be used to target end-users. As web browsers are also software, the same methods used to protect software would be implemented to mitigate threats to the web browser. It should be noted that web browsers also make use of third party software to enhance the end user experience (Barth, Felt, Saxena & Boodman 2010). Examples of third party software are Acrobat Reader, Java and Acrobat Flash. All web browsers and third party software should be updated regularly to mitigate the threat that targets web browsers.

Web browsers are mostly used for sending of emails, visiting websites and networking with other users on social networking sites. These computer uses are aligned with the uses identified in Sections 5.2 and 5.3. These three uses are added to the web browser node within the attack tree and mapped against threats as identified in Sections 5.2 and 5.3.

From a practical point of view, accessing the majority of services on the Internet requires authentication. Thus, password management is added to the threats identified in Section 5.2. Also, the threats originating from social networking sites (as identified in Section 5.3) are added to the listing of threats. For example, evil twin attacks, cyberbullying, fake profiles and privacy were identified as threats against end users as these threats originate from social networking sites.

Email services could be used by cybercriminals to target unsuspecting users with spam, scams, phishing and malware. Most of the messages received via this medium are designed to entice the user to open the email or click on a link, and thus social engineering is added. In addition, users who frequent websites are also exposed to threats including malware and phishing. These threats targeting end users are mapped against the attack vector, which subsequently results in an attack tree as depicted in Figure 5-8.

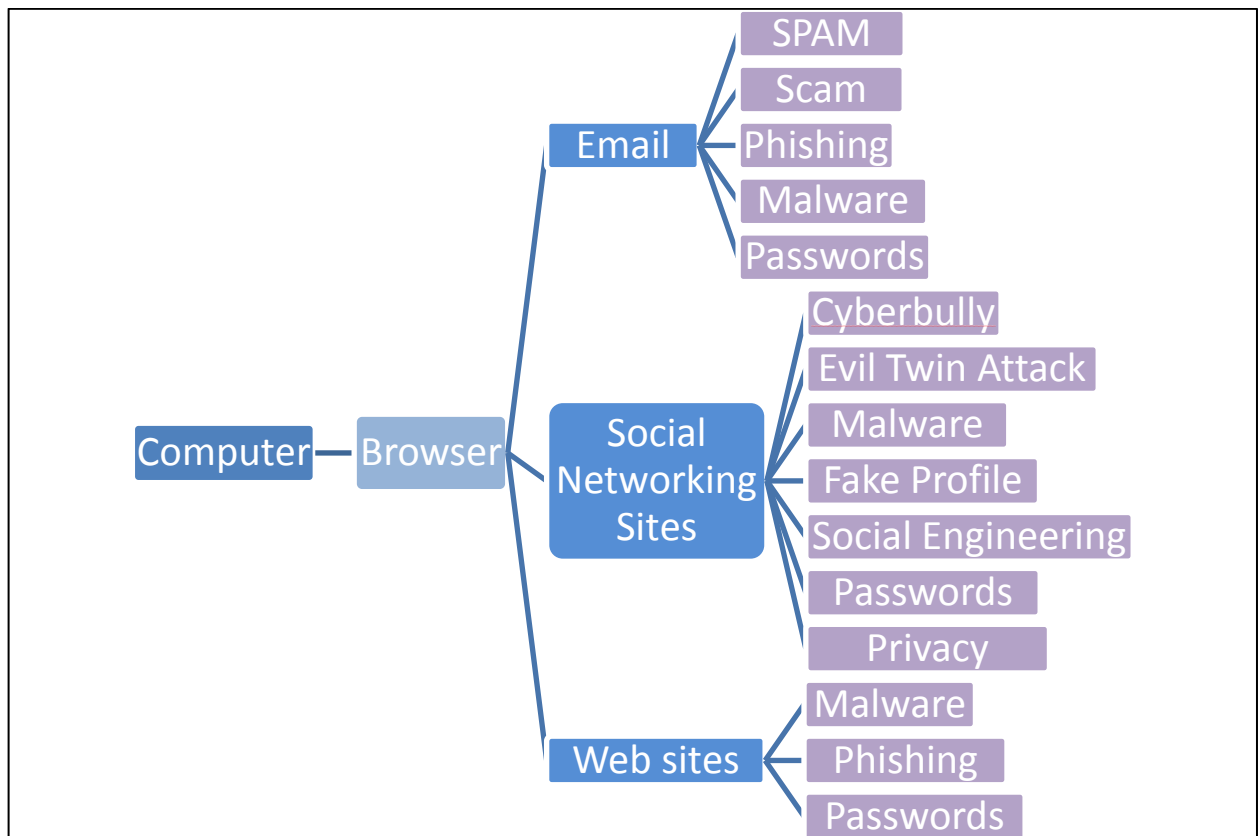


Figure 5-8: End User Attack Tree (Source: Own)

All the topics identified through the use of the attack tree were grouped together into high level categories which encompasses the threats identified. The following categories which cover all the topics were considered for the information security awareness program to be used within this study:

- Malware
- Social Networking Sites
- Phishing
- Spam
- Web Browsers
- Passwords
- Cyberbully

## 5.5 Conclusion

The previous chapter identified the different components which form part of the NIST information security awareness framework. This chapter addressed the application of the

design phase of the NIST information security awareness framework in this research. An assessment was conducted within a shared resource environment and within social networking platforms to identify needs and subsequently potential topics to be used within an information security awareness program.

The literature study on Internet Cafés proved beneficial in the identification of threats targeting novice end-users. These users make use of resources to access the Internet without considering security concerns, which could be attributed to lack of knowledge and skills on the topic of information security. Some security controls could be delegated to external entities due to the complexity when implemented. For example, a shared resource environment could ensure that the computers are not compromised by malware and can withstand a network attack. This could be achieved by hardening the operating system against threats with regular updates and installing anti-malware tools (which include anti-virus suites). The literature study resulted in the identification of different routes also known as attack vectors targeting novice computer users when accessing the Internet.

In addition, an experiment was designed, developed and implemented to determine the threats originating from social networking sites. The experiment focused on the ease of collecting data published by users on these platforms and using this data for nefarious purposes. This chapter also addressed one of the stated research objective questions. Section 5.3 addressed the research question “*What is the current security knowledge of information security novices?*” The experiment highlighted the improper use of security controls within social networking sites resulting in the leaking of personal information. This underlines a need to improve the awareness of novice users on the topic of social networking security.

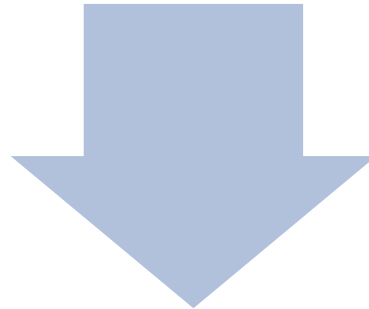
The next chapter describes the development phase of the NIST framework, which addresses the development of the information security awareness program. This phase involves the identification of the topics which form part of the information security awareness program. Additionally, the information security awareness program requires an effective platform to deliver the content of the selected topics (thereby addressing the need identified in this chapter). Two platforms are considered for the effective delivery of the information security awareness program. The Shared Public Security Awareness (SPSA) System and online gaming are design considerations described as part of the development phase of the NIST framework. The availability of an effective delivery

platform is critical to the success of the information security awareness program used within this study.



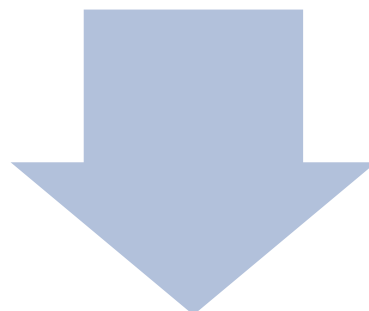
## Chapter 6: Development (Distribution Platform)

Chapter 5 - Design of Information Security Awareness Program



### Chapter 6 - Development (Distribution Platform)

- 6.1 Introduction
- 6.2 Shared Public Security Awareness System
- 6.3 Design Consideration of Information Security Awareness Program through Gaming
- 6.4 Conclusion



Chapter 7 - Implementation (Data Collection)

Figure 6-1: Layout of Chapter 6

## 6.1 Introduction

The previous chapters discussed the importance of security and how information security awareness is a critical component in equipping home end users with information security knowledge to mitigate the threats posed by cybercriminals. These chapters also covered the different components of the NIST information security awareness framework, which include the design, development, implementation and evaluation phases for an information security awareness program. Chapter 5 focused on the design phase of the NIST information security framework, which resulted in confirmation of a need (and identification of the topics) for an information security awareness program.

This chapter addresses the development phase as prescribed by the NIST framework. The required outcomes resulting from the development phase include the selection of topics, and the identification of methods to disseminate the knowledge to the intended audience. This chapter first proposes a framework for an automated information security awareness system, which could deliver the content of the identified topics to the potential users.

The proposed system can be deployed in an Internet Cafés within a rural area and provide information security awareness to the users at any given time. This system could be used to determine the information security awareness levels within a selected area, or conduct an information security awareness training without a trainer, since it is web based and uses a robust Internet portal system. The chapter then describes the design requirements for the data collection component of the automated information security awareness system. A prototype was developed from the design requirements to test the functionality of data collection component.

The resulting design consideration, together with the prototype feedback, would be used to develop and implemented an online game as part of the third phase of the NIST information security awareness framework. The online game would collect data, to determine its effectiveness, but also transfer knowledge to the participants of the information security awareness program.

Section 6.2 discusses the system components. The Awareness Collection System to be used within this study is explained in Section 6.3.



## **6.2 Shared Public Security Awareness (SPSA) System**

This section describes the design of a platform consisting of multiple components, resulting in an integrated system to deliver an information security awareness program. The content of information security awareness programs can be delivered to the intended audience through various delivery tools which include computer-based training (CBT), posters and screensavers to name but a few. In some cases these tools are combined: for example, the distribution of newsletters covering information security awareness topics can be handed out during in-person training sessions within companies that enforce information security awareness training.

The execution of such a program requires the appointment of staff who would conduct the in-person training, which would incur costs for example billable man hours to carry out the training. Additional expenses might include travelling, in the case whereby the trainer needs to visit a remote location. The impact of the training needs to be monitored as a means to determine the effectiveness of an information security awareness program and the expenses incurred has the required results.

These mentioned requirements are feasible within a well-funded environment, but not all end users have access to these vital programs. Subsequently, a need has been identified for the development of an autonomous information security awareness platform. This proposed platform could be deployed at establishments like Internet Cafés to automatically conduct the information security awareness program. This would benefit the owners of these establishments as well as end users who use the resources. Thus, design considerations should include threats encountered at establishments which allow multiple users to access the Internet from the same resources.

It should be noted the proposed platform discussed in this section could also be used within other environments where end users access the Internet. The main focus is the development of an effective information security awareness tool.

The remainder of Section 6.2 describes the design of an automated information security awareness platform, which delivers the content and monitors the effectiveness of the program. Section 6.3 focuses on the data collection component within the information security awareness platform, which primarily will be used for this study.

### 6.2.1 Requirements

End users who use shared resources or do not have access to information security awareness programs could visit establishments that deploy an autonomous platform which provides those services.

Such a platform provides several advantages:

- No additional human resources or intervention are required to conduct the information security awareness program.
- The platform could automatically conduct an information security awareness program.
- Data collected by the autonomous platform could determine the effect of the information security awareness program.
- Identify user behaviour which could be detrimental to their security.
- Provide a secure environment for each end-user session.

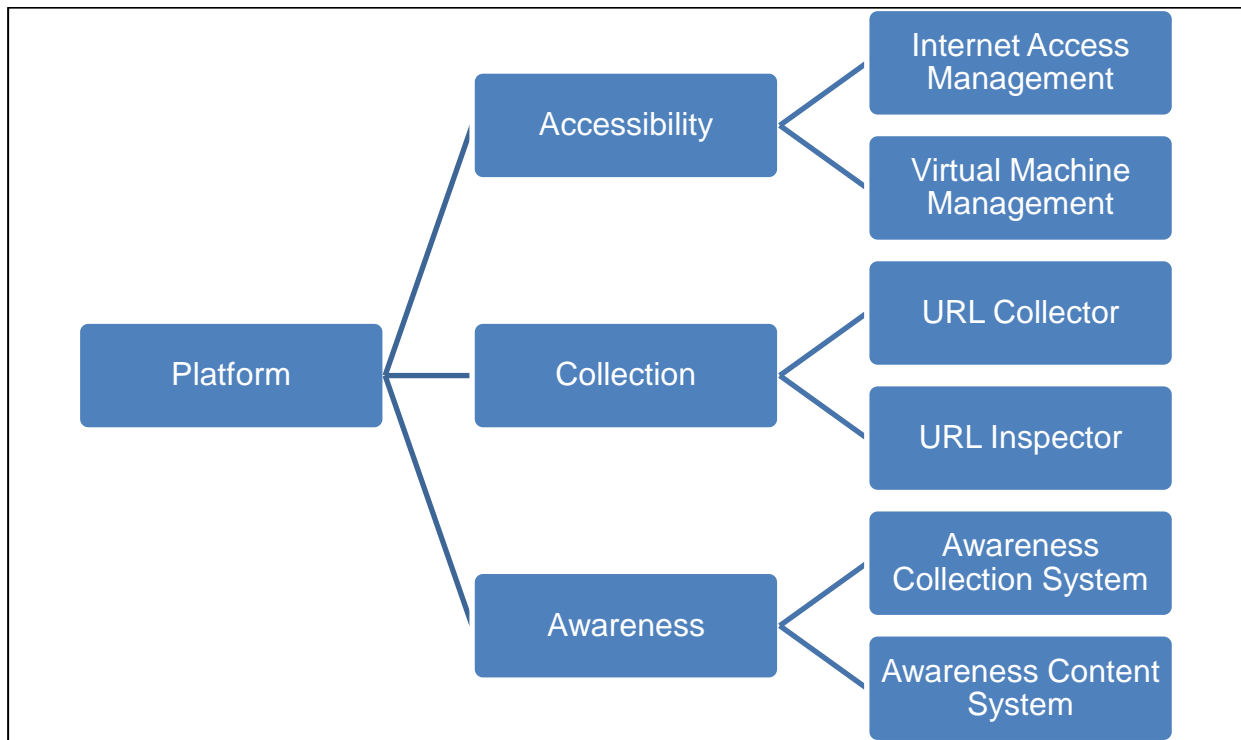
Such a platform should adhere to the following requirements:

- A robust and automated architecture which ensures availability and configurability of the system. This is achieved with the implementation of virtualisation and customisation of existing systems.
- The identification of threats that originate from users visiting malicious websites.

The platform should have the following capabilities (See Figure 6-2):

- Accessibility – Ensures that vetted users have access to the Internet. The vetting process ensures the users are authenticated and have an acceptable level of information security awareness. The effects of malware infections are minimised through the use of virtual machines, with the added benefit of limited downtime in the event of a malware infection.
- Collection – The collection component operates as an Internet usage tracking system. This provides data about possible effects of the information security awareness program such as a decrease in visiting malicious sites after attending an information security awareness program that focused on malicious links received via emails.

- Awareness – The awareness component provides the functionality to determine the current information security awareness of the users, and also conducts information security awareness training.



**Figure 6-2: Capabilities of Shared Public Security Awareness System (Source: Own)**

These capabilities would allow the platform to achieve the stated requirements. The platform could also be extended to conduct automated information security awareness programs and collect data to determine the effectiveness of the program.

Sections 6.2.1.1 and 6.2.1.2 describe methods for implementing the stated requirements of the Shared Public Security Awareness (SPSA) System.

#### **6.2.1.1 Virtualisation, Automation and Customisation**

The SPSA system's underlying architecture consists of virtual machines. Bell (2011) defines a virtual machine as software that functions as a computer without physically being a computer. The use of virtual machines involves creating a baseline state. Thereafter, changes that occur during use can be reverted, restoring the virtual machine's original configuration. This is useful in environments where computer systems are exposed to external threats, as in the case of Internet Cafés or any other establishment that allows end users to connect to the Internet. In the event of a security breach, the virtual machine

can be reset, resulting in less downtime for the end user as the computer does not need to be reinstalled.

The use of virtual machines as a security measure is also noted by England and Manferdelli (2006), who propose a model for deploying virtual machines in order to secure the enterprise desktop. For example, one computer might be used to conduct normal duties while classified work would be done on another computer not connected to the network; in this case, the segregation of the computers increases security. However, this is not cost effective as the number of assets, namely computers, would need to be procured to accommodate the requirements. The use of virtual machines could be cost effective and improve security as compromised systems could be reset to the original state. Also, some variants of malware do not execute within a virtual environment, as the malware authors are employing measures to prevent the security community from analysing the malware and developing techniques to mitigate the threat (Zhu & Chin 2007).

The lifecycle of the SPSA system starts with the creation of a baseline virtual machine, which is considered to be secure and thus not compromised. A copy of this virtual machine is created and loaded for daily use. This ensures end users have a trusted platform to use. At the end of the day, the virtual machine is dated and stored for analyses. Research teams could analyse the virtual machines for threats that compromised the virtual machine, resulting in an understanding of the attack vector used by cybercriminals. This process is also recommended by Harlan (2005), who described the malware analysis cycle with the use of virtualisation. The ability to restore to a useable state is critical in places where the business model is built around customers using resources to perform activities, as in the case of Internet Cafés. Computers at Internet Cafés are provided to end users to access the Internet for a fee and if a computer is compromised and cannot be used, then the business bottom line is affected. The use of virtual machines could decrease the downtime as any compromised virtual machine only needs to be restored to its baseline state.

One of the capabilities requires the platform to be automated. This would allow the platform to operate autonomously. The use of virtual machines has the benefit of scripting, resulting in:

- Starting the virtual machine at a predefined time,
- Creating a backup,

- Loading a new virtual machine image.

The SPSA system has a dual function as described earlier in that it not only has the ability to conduct an information security awareness program, but it is also a means of access to the Internet. The use of existing open source Internet access management systems would allow for customisation. Easyhotspot (Awan 2007) is a hotspot billing system released under a general public license (Stallman 1991), which implies that the software could be modified without prior permission from the original application team to develop the SPSA system from the requirements.

The Easyhotspot system is depicted in Figure 6-3. An implementation could allow the SPSA system to determine which features to present to the end user, for example the end user could be directed to the information security awareness program for remedial work if the user does not have a high enough information security awareness rating. Another implementation could be to present information security awareness-related content to the end user before they access the Internet, as a measure to remind them of safe practises to prevent falling prey to cybercriminal tactics. Kruger and Kearney (2006) recommend continuous exposure to security-related content as it contributes to the success of an information security awareness program.



Figure 6-3: EasyHotspot Management System (Awan 2007)

The next section describes an additional use of the SPSA system, namely the need to determine the effectiveness of the information security awareness program by collecting and analysing data generated by the end users.

### **6.2.1.2 Threat Collection and Analysis**

One of the key components of the SPSA system is the ability to conduct security analysis on the virtual machines and Internet data to determine if the users were compromised during their sessions on the Internet. Cybercriminals have adopted sophisticated techniques to entice end users in an attempt to influence them to perform actions which could be detrimental to their security. For example, social networking sites have increasingly been adopted and used as part of daily life. Cybercriminals have also noticed the trend and adopted their strategies to include social media malware. Work conducted by Abraham and Chengalur-Smith (2010) on social engineering malware indicates attackers utilise numerous avenues which include websites, social software and email for infection. All these avenues are accessed via web browsers. Subsequently, the data generated when visiting websites requires analysis to identify threats and the effectiveness of the information security awareness program. In other words, the SPSA system needs to visit the same websites the users visited to determine if any threats exist. Also, if the information security awareness program covered topics about visiting malicious websites, then the system must adapt and direct the user for remedial work on the topic of safe website usage in the case where a user tries to visit such a malicious website.

The URL is one of the data components which would be analysed. Polychronakis et al. (2008) proposed the design of a URL collection system used in exploring the life cycle of web based malware. The system analysed the web pages for malicious content. This was achieved by visiting the URL and monitoring the system for new processes, files system changes and registry modifications. Provos (2007) also proposed a similar approach which consisted of identification of URLs, in-depth verification of maliciousness and aggregation of malicious URLs into site level ratings.

Another component to be analysed is the content on the website, which could be achieved with the use of a programmable web crawler. Mohr, Kimpton, Stack and Ranitovic (2004) discussed Heritrix, which is an open source extensible, web scale, archival-quality web crawler. Ikinici, Holz and Freiling (2008) demonstrated the effectiveness of Heritrix as part of the MonkeySpider system which is used in the detection of malicious websites.

The following section discusses the architecture of the SPSA system. The identified requirements are achieved through the development of the functional components of the SPSA system. Together, these components provide the SPSA system with accessibility to the Internet, collection of data and the ability to conduct an information security awareness program autonomously.

### **6.2.2 Shared Public Security Awareness (SPSA) System Architecture**

The SPSA system consists of multiple components which are used for various functions. These functions provide the required capabilities as discussed in Section 6.2.1 and depicted in Figure 6-2. These functions could be used independently, as in the case of providing only Internet access or conducting only an information security awareness program. The following sections discuss these components as follows:

- The automated virtualised environment is discussed in Section 6.2.2.1 and 6.2.2.2.
- Section 6.2.2.3 and 6.2.2.4 address the collection of browsing session data.
- Section 6.2.2.5 and 6.2.2.6 elaborate on the information security awareness program delivery mechanism.

#### **6.2.2.1 Internet Access System**

The first component of the SPSA system provides Internet access to the users. However, the system utilises a modified user management system, which allows the system to determine what component to activate for individual users. In other words, the system could allow a user to access the Internet if their information security awareness levels are calculated to be above a selected threshold. The system could also direct the user to a security awareness program for training until the user has attained the required information security awareness level. This workflow is depicted in Figure 6-4.

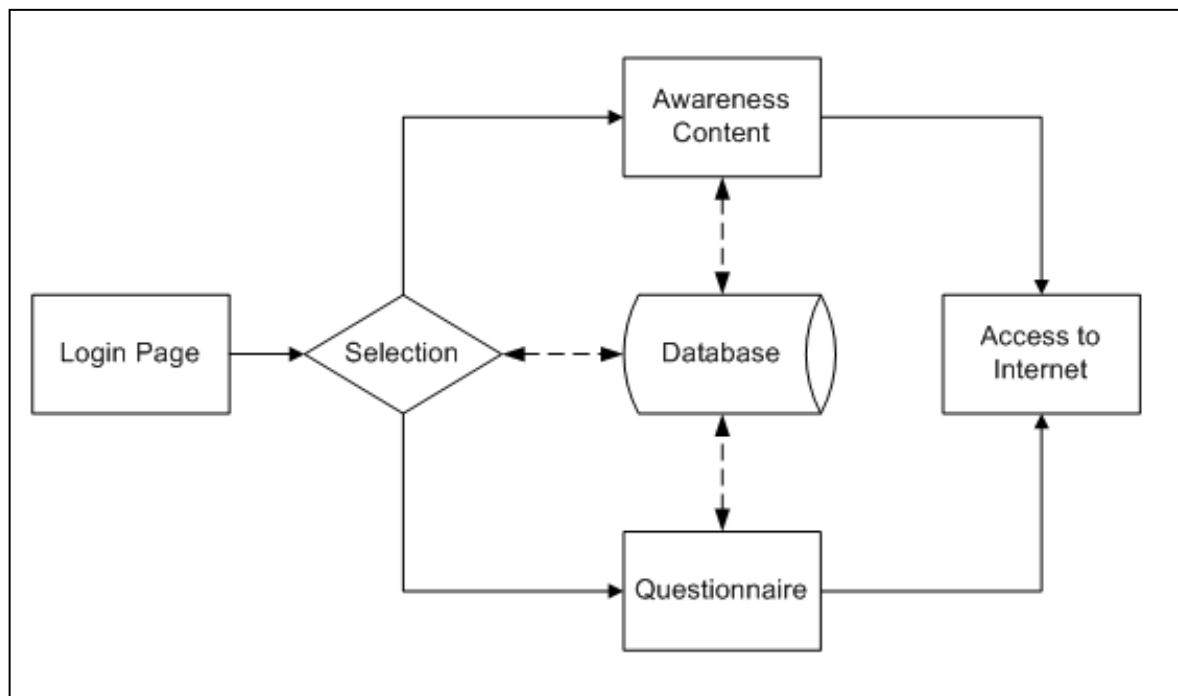


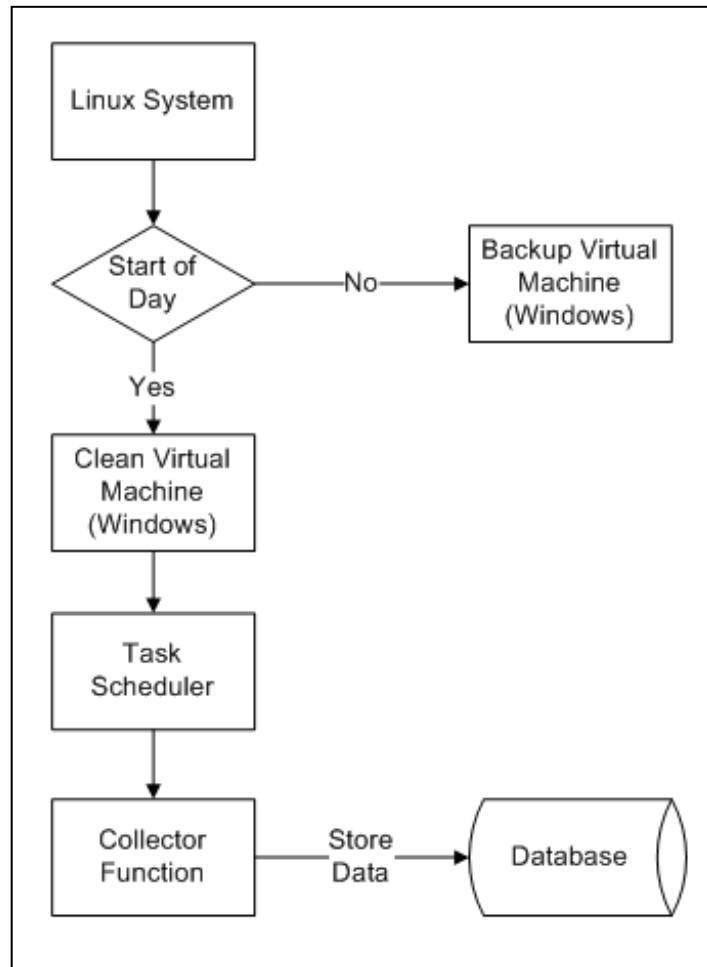
Figure 6-4: Internet Access System (Source: Own)

In addition to the security rating evaluation, the security best practices would be displayed to the user before he or she would be allowed to access the Internet. This would serve as a reminder to the end user about potential threats they could encounter online.

### 6.2.2.2 Virtual Machine Manager

As described in the requirements section (Section 6.2.1.1), the use of virtualisation as part of the SPSA system is critical in the deployment of an autonomous system. The Virtual Machine Manager automates the process of deploying a virtual machine for daily use at the start of the day and creating backups of the virtual machine used during the day. The virtual machine image deployed at the start of the day is classified as the baseline, which implies the system is not compromised. This is verified by running software to determine if the system has malware infections and ensure that all software is up to date. The backup version is stored for analysis to determine if a user's behaviour has compromised the system. The workflow is depicted in Figure 6-5.





**Figure 6-5: Daily Virtual Machine Operations (Source: Own)**

In addition to the start-up and loading of the virtual machines, other scripts on the virtual machines will be initiated by the task scheduler. The scheduler initiates the scripts to collect the URLs and store the data in a database while the end user is visiting websites, which is discussed in the following section.

### **6.2.2.3 URL Collection System**

Several threats originate from the use of web browsers. The uniform resource locator (URL) Collection System collects website addresses as the end user accesses the Internet. This occurs seamlessly and thus, it does not interfere with the browsing experience. This collection is initialised once the virtual machine becomes active. A network protocol analyser is used to extract the URL from the web traffic. According to Forouzan (2003), “*The URL is a standard for specifying any kind of information on the Internet*”. In other words the URL refers to the address of a web page.

The URL provides a route to the content that was accessed by the user. TShark has been used in several studies for the collection of specified network traffic (Nascimento & Correia 2011, En-Najjary & Urvoy-Keller 2010). En-Najjary and Urvoy-Keller (2010) proposed statistical classifiers for unencrypted and encrypted internet traffic to identify application within enterprise networks. The work conducted by Nascimento and Correia (2011) focused on the data generated by an intrusion detection system within a production environment. In both of these cases the collection of network traffic was through the use of a network analyser named TShark.

The data collection for the URL Collection System is actualised by a custom developed implementation using TShark within the SPSA system. The collected data is stored in a file and subsequently transported to be stored within a database. The analysis of the URLs is conducted by the URL Inspector, as described in the following section.

#### **6.2.2.4 URL Inspector**

The examination of the collected URLs is conducted by the URL Inspector. The main objective of the URL Inspector is to determine if the sites visited by the end users contain any malicious software which could have compromised the computer system. The workflow is depicted in Figure 6-6. The URL Inspector consists of two components:

- **URL Analyser** – Determines if the site visited is identified as a malicious site by Google. The URL Analyser will examine each collected URL in the database against the Google Safe Browsing database, a service provided by Google which enables applications to examine the location of the website against known phishing and malware websites (Google Code Lab 2015).
- **Malware Collection and Classification (MCC)** – Determines if content on the website classified as malicious by an anti-virus software vendor (ClamAV). The system consists of an Internet crawler called Heritrix which will be used to download the content from the URL and store the result data set in an archival format (ARC). Subsequently the ARC files will be forwarded to ClamAV which in turn will be used to determine if the content is malicious.

The results from both these components are encapsulated in a report which could be used to determine the effectiveness of the information security awareness program, as well as identifying the threats which could be targeting end users using a web browser.

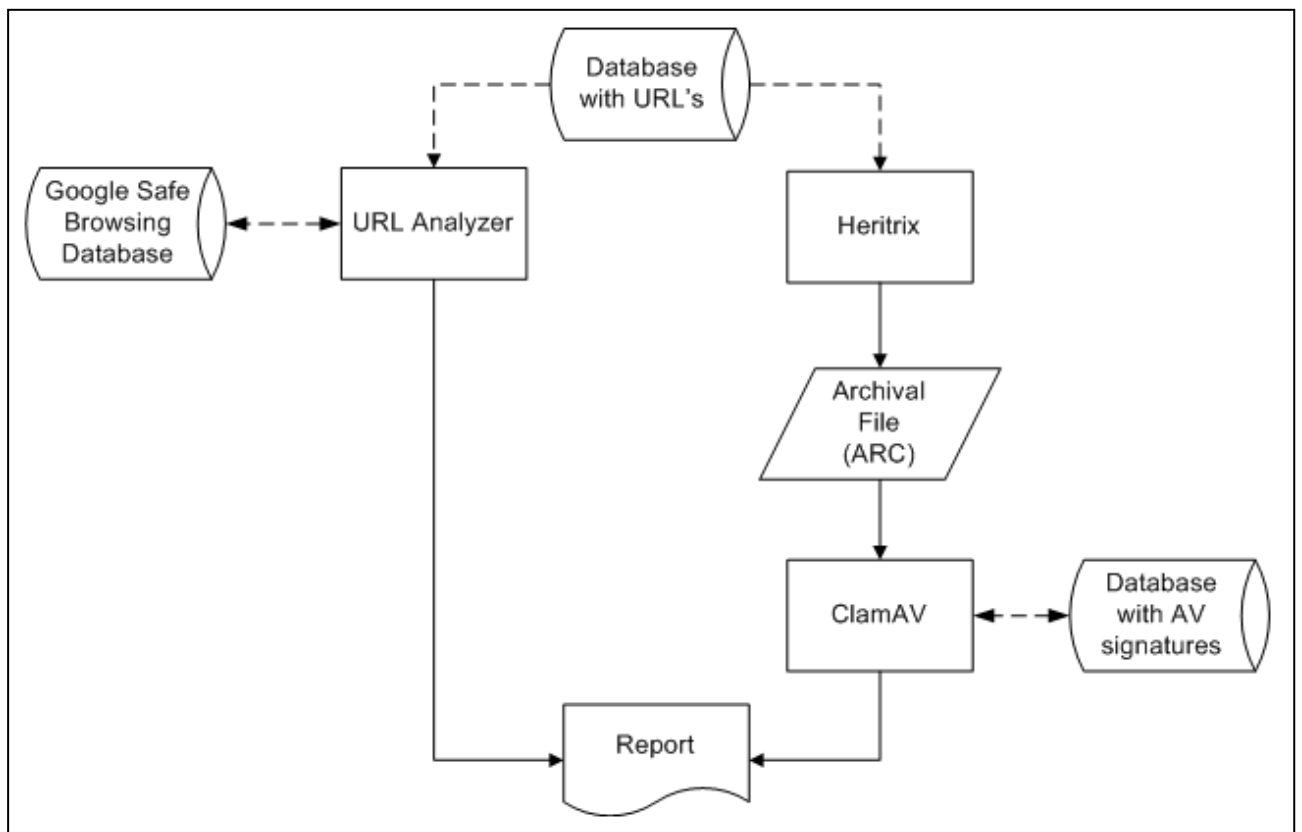


Figure 6-6: URL Inspector (Source: Own)

The following section describes the collection of data, focussing on the information security awareness component of the SPSA system.

#### 6.2.2.5 Awareness Collection System

One requirement of the SPSA system is to conduct an information security awareness program, but another is to assess the information security awareness level of an individual who is accessing the Internet via the system. The awareness level forms part of one metric to determine the effectiveness of the information security awareness programs. The SPSA operates autonomously and thus the system requires data to respond programmatically to the required Internet access configuration described in Section 6.2.2.1.

Users' information security awareness levels are measured with the use of questionnaires, which focus on threats that target end users accessing the Internet. Wilson and Hash (2003) discussed best practises for information security awareness programs and subsequently proposed a comprehensive list of awareness topics, which include but are not limited to:

- Password usage and management

- Spam
- Social Engineering
- Web usage
- Shoulder surfing
- Desktop security
- Unknown e-mail/attachments
- Incident response

A rating is assigned to each end user who completed the questionnaire on the SPSA system. The Internet access management system grants access to the end user if the rating is higher than the required rating, or redirects the user to the information security awareness program which provides information about the topics, as described in the following section (See Section 6.2.2.6). All the end user ratings can be compiled into a report that indicates the areas of concern and identifies the topics that need to be addressed by the information security awareness program. These results could also be incorporated in to the E-Awareness Model (E-AM) proposed by Kritzinger and Von Solms (2010). This model would not allow home users to access the Internet if their information security awareness levels are not satisfactory. Also, the users are required to complete remedial work to address the shortcomings before access to the Internet is granted.

The Awareness Collection System should be developed using gaming design principles as this would improve the user experience while collecting valuable data to determine the information security awareness rating of the end user. Game play encourages learning and with the use of game play components, users are enticed to return to continue with the game. Priebatsch (2010) recommended the use of the following dynamics to form part of game play:

- **Appointment** - The appointment dynamic calculates consecutive logins over a period for the user. The user has to ensure that they continue using the system after the badge has been obtained.
- **Influence and Status** - The status badge is provided when a user answers a number of questions correctly. Therefore, the user is encouraged to provide the correct answers

- **Progression** - The progression dynamic is represented with the progress bar which provides the user with a visual indicator on progress.
- **Communal Discovery** – This dynamic allows several users solve problems together however this dynamic is not considered for this research and does not form part of the game used within the Awareness Collection System.

These dynamics are demonstrated visually with the use of badges. A badge is a visual indicator of an achievement. A proposed graphical user interface is depicted in Figure 6-7.

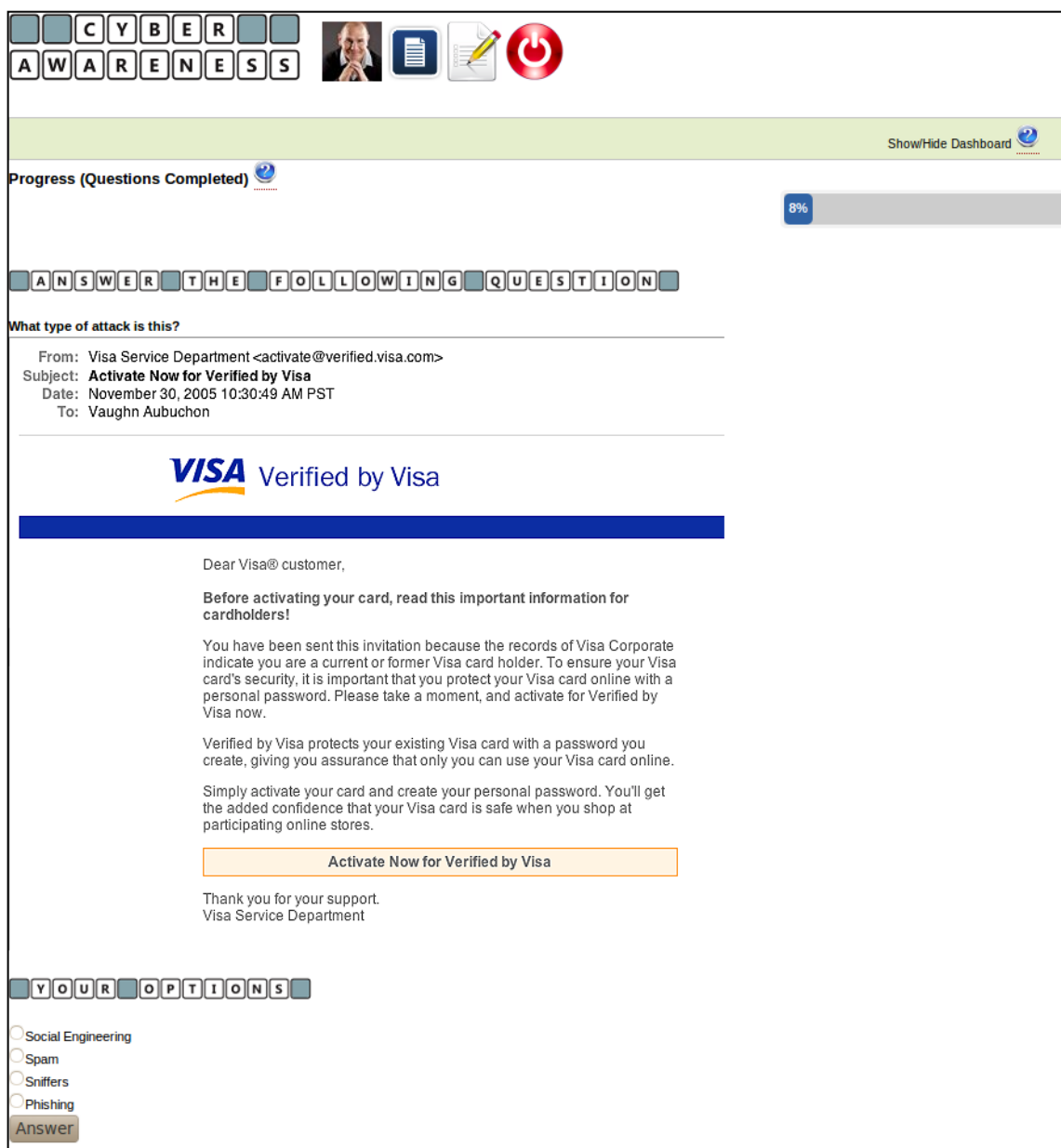


Figure 6-7: Awareness Collection System (Source: Own)

This section discussed the components used within the SPSA system to determine the information security awareness level of users. The next section addresses the Awareness Content System that focuses on providing a capability to transfer knowledge about the identified security topics to the end users.

#### **6.2.2.6 Awareness Content System**

The final component of the SPSA system delivers information security awareness topical content to the end users. The previous section described the component which determines the information security awareness level of an individual end user. If the user's rating is not high enough, the SPSA system directs the user for remedial work. Remedial work consists of the end user acquiring additional knowledge on the related topics.

As in the case of the other components, the requirement for customisation can be achieved with the use of a content management system (CMS), for example Moodle, which is software package for producing Internet-based courses and websites (Dougiamas 1999). Some typical features of Moodle are assignment submission, a discussion forum, file storage, grading, instant messaging, an online calendar, news and announcements blog, online quizzes and a wiki. These features provide a platform that integrates the requirements of the SPSA system in the delivery of information security awareness content and mechanisms for assessment. The CMS stores the material of the identified information security awareness topics, which the user can then easily access. New topics can be easily added to the current list. Typically, a standard format of the content should be followed when new content is added. A suggested format includes the following:

- Background information
- Identification of the threat
- Mitigation techniques
- Links to additional resources

For example, one topic addresses the dangers of shortened URLs, which could be encountered on social media platforms (Figure 6-8).

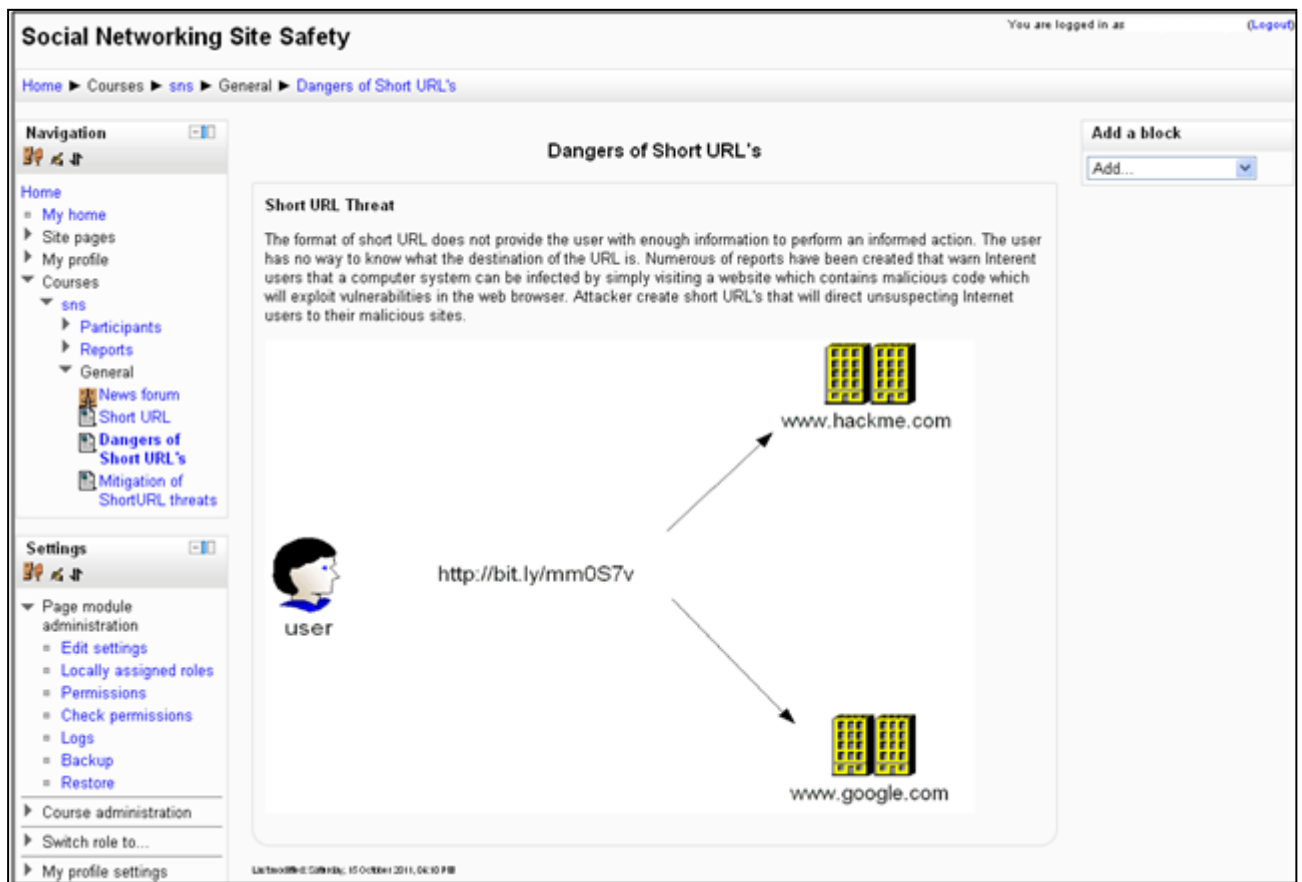


Figure 6-8: Awareness Content System (Source: Own)

### 6.2.3 Conclusion

This section proposed an information security awareness system to autonomously provide information security awareness training, which could be effective in areas where end users do not have access to this important knowledge. The system contains many components, which include the provision of a robust platform allowing users to access the Internet, quick recovery in the event of a malware infection, tracking of Internet behaviour (which could be used as a metric to support an effective information security awareness program), and the capability to automate the delivery of an information security awareness program.

Although the information security awareness program can be automated, it is essential to ensure that knowledge is transferred and learning has taken place. A need is identified to ensure that information security awareness knowledge is maintained after the completion of the training program.

As the NIST development phase requires the identification of a tool to conduct an information security awareness program, this section has proposed the development of

such a tool. However, the game component of the SPSA system and its possible effectiveness is the focus of this study. The next section investigates the use of game play as a mechanism to enhance learning of the information security awareness content.

### **6.3 Design Consideration of an Information Security Awareness Program through Gaming**

The previous section proposed the SPSA system, which automates the delivery of an information security awareness program. Although the system can be automated, the need arises to ensure that knowledge transfer occurs and learning takes place, and to ensure that the newly acquired knowledge is not forgotten. In other words, the users should not forget what they learned. Numerous techniques exist to transfer knowledge to the participants of the information security awareness program including posters, web based and in-person training sessions to name but a few. However people learn differently and not all techniques may result in effective learning.

This section describes the design and development requirements for the Awareness Collection component of the SPSA system. This component would not only collect data, but would also be used to deliver the content of the information security awareness program through the use of online games. This section determines the requirements used in the design of online games. The use of games to improve the effectiveness of an information security awareness program is also described here. The resulting design considerations are used to develop an online game to deliver the content of the information security awareness program.

Section 6.3.1 provides the motivation for game design. The requirements of effective game play components are described in Section 6.3.2. Section 6.3.3 proposes the design of a prototype online game as the delivery method for information security awareness programs used in this study.

#### **6.3.1 Gaming Motivation**

Numerous platforms are available to transfer knowledge from a source to a target group, as in the case of information security awareness. Many of these platforms are one-directional communication: in other words, the knowledge is only transferred from one end of the communication channel to the other. Albrechtsen and Hovden (2010) identified the following forms of one-directional communication: pamphlets, emails, intranet pages, screen savers, posters, mouse pads, pens, formal presentations and training sessions.



They also asserted that the effectiveness of the information security awareness program could be increased by having bi-directional communication, as the target group is actively involved in the understanding of the knowledge transferred. The added benefit of having input from the participants is that their input demonstrates understanding of the topic under discussion.

The importance of information security awareness programs have been noted by Kumaraguru, Sheng, Acquisti, Cranor and Hong (2010); Eminağaoğlu et al. (2009); Dodge (2007); Kumaraguru, Rhee, Acquisti, Cranor, Hong, and Nunge (2007) respectively. These are briefly listed as follows:

- Kumaraguru et al. (2010) demonstrated the effectiveness of using web based material in combating phishing attacks. An important observation from the study is the impact of using text and graphics to improve learning.
- Eminağaoğlu et al. (2009) showed that weak password usage was significantly decreased and users continually improved their awareness and complied with policies after attending an information security awareness training course.
- Dodge (2007) showed the reduction of victims by repeating an information security awareness program focussing on phishing attacks.
- Kumaraguru et al. (2007) found the use of concrete examples is best suited to convey abstract information. This was best achieved through the use of comic strips. They also found providing instructions to the participants while solving a problem was more effective.

These studies have clearly shown the effectiveness of information security awareness programs. However, this study focuses on the effectiveness of gaming as a platform and the identification of which components are required to improve the transfer of knowledge. It should be noted that the proposed autonomous information security awareness system described in Section 6.2.2.1 provided users with Internet access through the use of a web browser. Audio, video and animation formats can be used within the web environment. These multimedia formats could be used together to reflect real scenarios of information risks, as argued by Shaw, Chen, Harris and Huang (2009). They also raised the issue that information richness of different forms of multimedia can affect the effectiveness of online information security awareness programs. They have identified the following forms of

media which influence the richness of the information and subsequently have an impact on the effectiveness of the information security awareness program:

- **Hypermedia:** an interactive medium that consists of graphics, audio, video, plaintext and hyperlinks, which makes it the richest medium of the three. Concepts can be arranged visually and not sequentially to help users understand critical concepts and their interrelationships.
- **Multimedia:** combines text, image, sound, music, animation, video and virtual reality but must be accessed in a linear sequence.
- **Hypertext:** does not incorporate feedback, language variety, multiple signals or personal focus.

Shaw et al. (2009) concluded that hypermedia and multimedia were more effective in enhancing users' comprehension and projection ability of information security awareness, while hypertext-based training was more effective than multimedia in enhancing users' perceptions of security risks. In other words, the more senses were involved in the knowledge transfer, the higher the understanding and retention of the knowledge. Awareness is merely raised through the exposure to information. This also indicates that the effectiveness of the gaming component could be influenced by the richness of the information presented to the participant of the study.

Cone et al. (2007) found that video games can be effective in basic information security awareness programs. Their study focused on a game called CyberCiege developed for the Naval Postgraduate School in the United States of America (2004). This game is a highly extensible game for teaching information assurance concepts and applying problem solving and critical thinking to different scenarios.

CyberProtect (Department of Defence (United States of America) 1999), empowers network administrators in a gaming environment to learn about the threats encountered within a network and provides them with mitigation techniques which could be applied a controlled environment. The graphical user interface of CyberProtect is depicted in Figure 6-9, which illustrates the richness of the information presented to the user. CyberProtect is an online game but does not use a social networking site as the delivery platform.

Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong and Nunge (2007) designed an online game called Anti-Phishing Phil which focused on transferring knowledge to the end-users on phishing attacks subsequently promoting secure behaviour. Their game design principles allowed users to reflect on their actions within a story based environment while applying knowledge acquired. They found the game positively affected the end-users who played the game.

All this research suggests that a gaming platform could be deployed within a web application environment as many remote users would be able to utilise the game if it is part of a social networking site. Social networking sites have numerous successful games like Farmville, Mafia Wars, and Farm Town (Park & Lee 2012). Social networking sites also provide an accessible portal which developers can use to develop and deploy games within the social networking environment. Another benefit of social networking sites is the extensive user base.

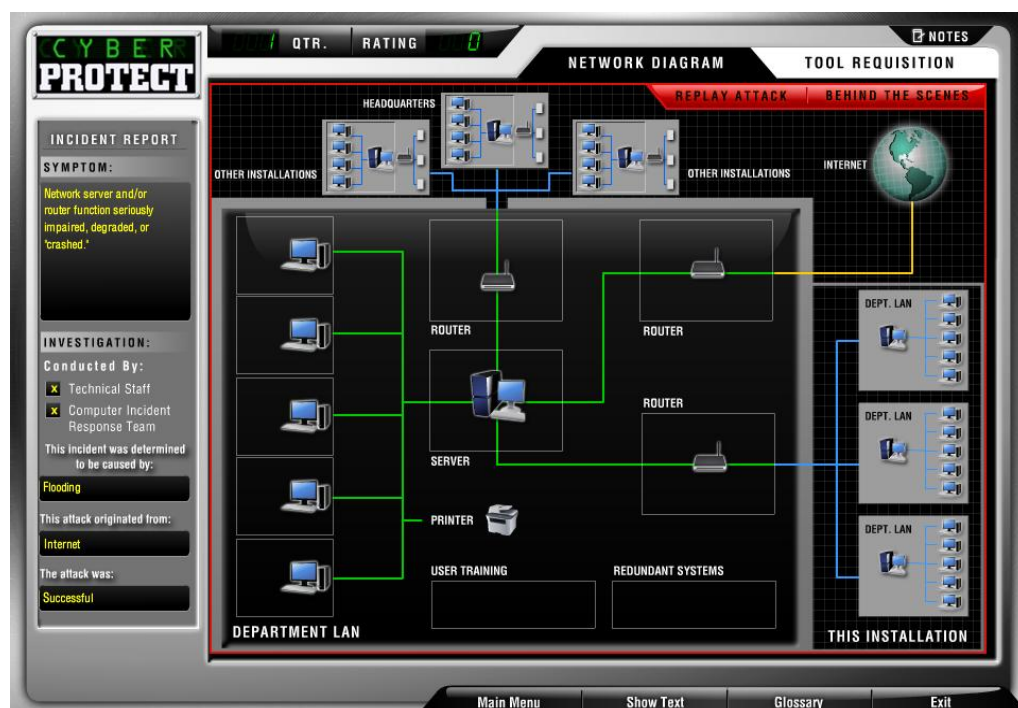


Figure 6-9: CyberProtect Interface (Department of Defence (United States of America) 1999)

This section motivated the need to use gaming as part of information security awareness program. The next section focuses on the design considerations for the game.

### 6.3.2 Requirements

This section conducts a literature study to identify the design requirements for the development of a gaming component as part of an information security awareness program.

Kruger and Kearner (2006); Hsu and Lu (2004); Shin and Shin (2011); Johnston, Eloff and Labuschagne (2003) and Priebatsch (2010) proposed design components that should be considered in the development of successful information security awareness games using social networking sites. This section summarises some key requirements that fed into the design of the information security awareness game, as depicted in Figure 6-10.



Figure 6-10: Game Design Requirement (Source: Own)

These requirements include the following:

- **A comprehensive database of questions** – The information security awareness levels of the participants will be assessed with the use of questions. As a measure to prevent repeating questions, a question bank should contain sufficient questions

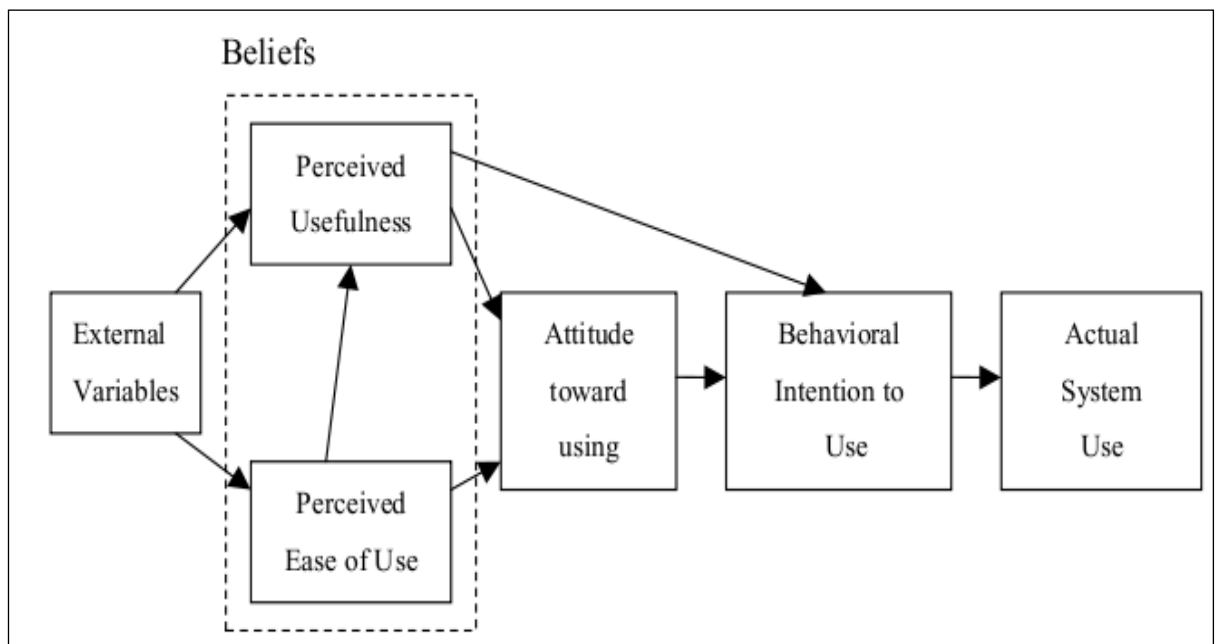
to avoid presenting the same question to the same user. Also, sufficient questions should be created on each topic to ensure the topic is covered in its entirety.

- **Weighting of the questions** – The question should be assigned different weights, each of which represents a difficulty rating. The use of a weighting system allows the system to determine the competency levels of the users on a certain topic. The difficulty rating also indicates the level of the challenge provided to the user.
- **The use of practical data** – It is imperative that the game uses information that resembles the environment or scenario expected to be encountered in practise. In other words, the data encapsulated in the questions should reflect real life scenarios that users can easily identify with. For example, discussing the concept and application of a Denial of Service (DoS) attack with an end user would not be effective. The user might barely understand the concept of password management, and the discussion of complex concepts might be detrimental to the motivation of the end user.
- **The tool should be automated** – The mechanism used to conduct the information security awareness program should be designed to function without the intervention and supervision of humans. The removal of the human component from the system suggests that the system can autonomously operate and allow multiple users from numerous locations to play the game simultaneously. This is an important component since social networking sites are Internet based, and allow multiple users to interact with the game.
- **Game dynamics** - All game design involves different gaming dynamics which incite users to come back and play again. Priebatsch (2010) discussed four game dynamics: Appointment, Influence and Status, Progression and Communal discovery dynamics. These were described in Section 6.2.2.5.
- **Easy accessible** – The users who intend to play the game require access without any obstacles as this might influence them negatively. Games developed to be executed on a single resource, like a laptop, only allow one user access to the game. This is ineffective and targets a small group of individuals. The study requires multiple users to have access in order to determine the information security awareness levels of both an individual and the group.

- **Effortless** – The end user interacts with the game through the use of an interface. This implies that the interface will influence the experience of the user. Nielsen (2005) lists critical factors for the design of the interfaces. These factors provide the users with an experience which builds trust with the application, increases productivity and reduces erroneous use (which frustrates the user). Nielsen proposes that the system status should always be visible to the end user – thus ensuring the user is informed of what is occurring within the system.

The end user should also be familiar with the system. In other words, the system should be a reflection of the user's real life. This can include localisation like using the same language as the end user. The user should be empowered to control the system without causing damage to the system. This also implies the system should prevent errors and provide users with help on how to recover from an undesired state. This can be achieved with the use of documentation or a help function. The design should be minimalistic and intuitive – thus decreasing the learning curve to use the system.

- **Acceptance by the user** – The Technology Acceptance Model (TAM) was originally proposed by Davis (1985). Furthermore, Moon and Kim (2001) states that TAM provides determinants of individual adoption and can explain and predict the individual's acceptance of Information Technology (IT). This is critical to end users who lack knowledge on the security topics defined within the realm of computer use, as these users might resist the exposure to security concepts. Figure 6-11 illustrates the different determinants of TAM as originally specified by Davis (1985). Users encountering new technology for the first time may question the usefulness and the ease of use of the new technology. Perceived Usefulness (PU) and Perceived Ease of Use (PE) affect the belief of a user, which influences the attitude towards using the technology and also affects the behaviour to finally use the system (Chuttur 2009).



**Figure 6-11: TAM Model (Davis 1985)**

TAM has been extended by Hsu and Lu (2004) to address online games (Figure 6-12). Two additional determinants have been added: Social Influences and Flow Experience. Social Influences have been identified to shape user behaviour through social norms demonstrated by other groups. People tend to look upon others' behaviour when faced with a situation where they do not know how to react (Cialdini 1998). Csikszentmihalyi (1991) defined the concept of flow as "*the holistic experience that people feel when they act with total involvement*". This definition suggests that flow consists of four components - control, attention, curiosity, and intrinsic interest.

Shin and Shin (2011) identified the need to adapt the TAM to accommodate social networking sites with the addition of the following determinants: Perceived Playfulness (PP) and Perceived Security (PS). These two determinants address the level of curiosity during an interaction with technology and the security concerns that has been raised with use of social networking sites. They found that PP was related to PE and PU. Therefore the determinants: PE, PU, PS, PP and flow are important factors that need to be reflected in the design of a game utilising social networking sites.

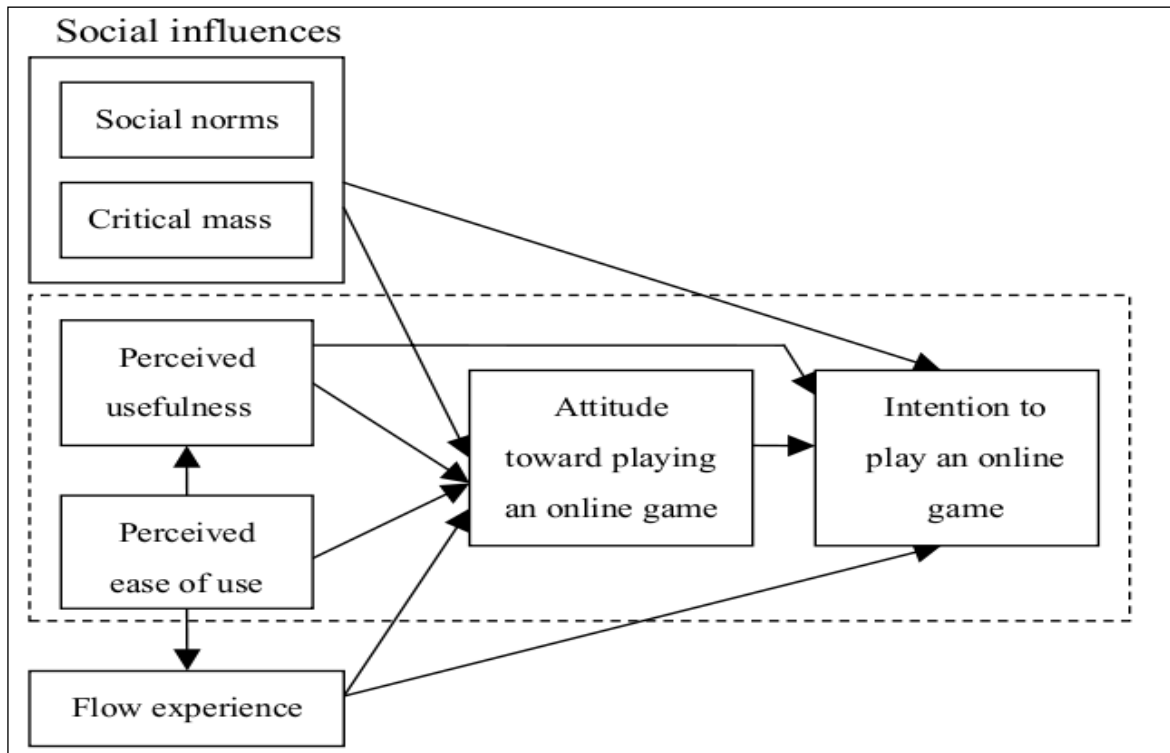


Figure 6-12: Extended TAM Model (Hsu & Lu 2004)

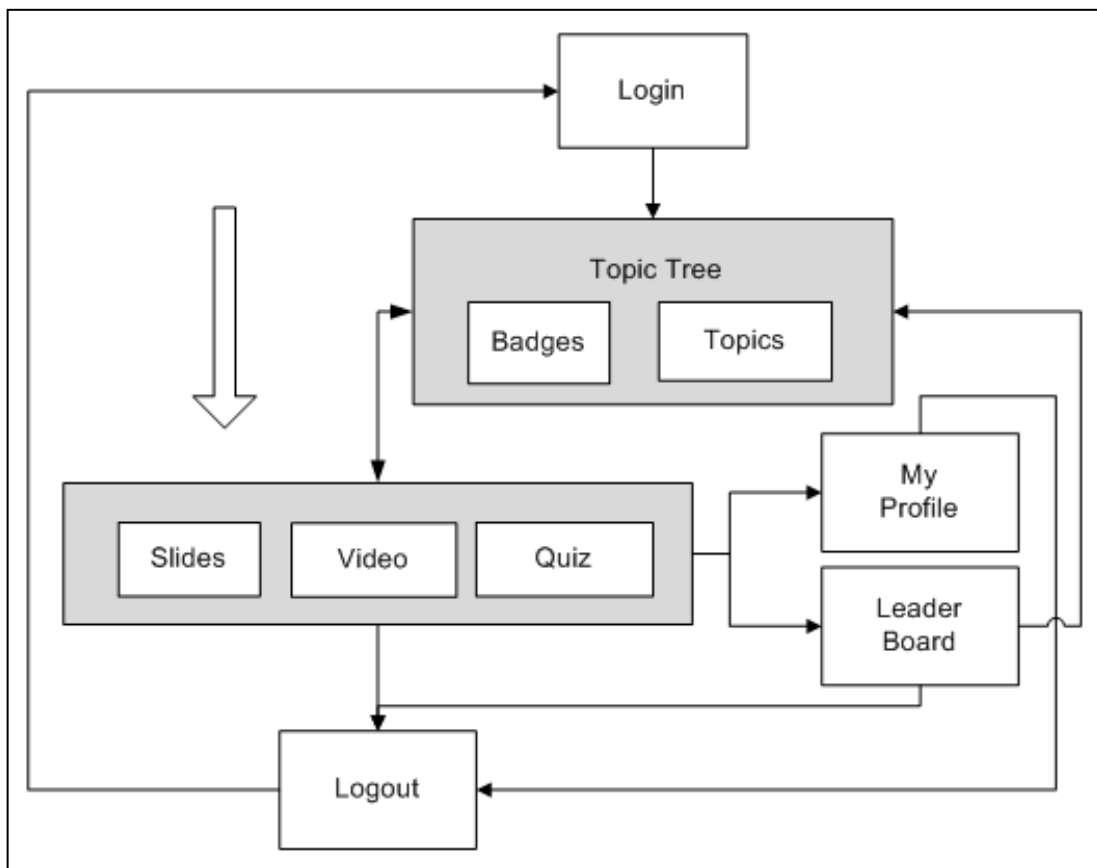
This section investigated the design considerations required for the design and development of a gaming component that could form part of an information security awareness program. The next section uses some of these requirements in the design of a prototype online game. This prototype serves as the initial step in the development of the game used within this study.

### 6.3.3 Conceptual Game Prototype

This section describes the proposed prototype for the gaming component. The design takes into consideration the requirements identified in the previous section. A conceptual design with partial implementation was conducted.

This high level design and flow is depicted in Figure 6-13.





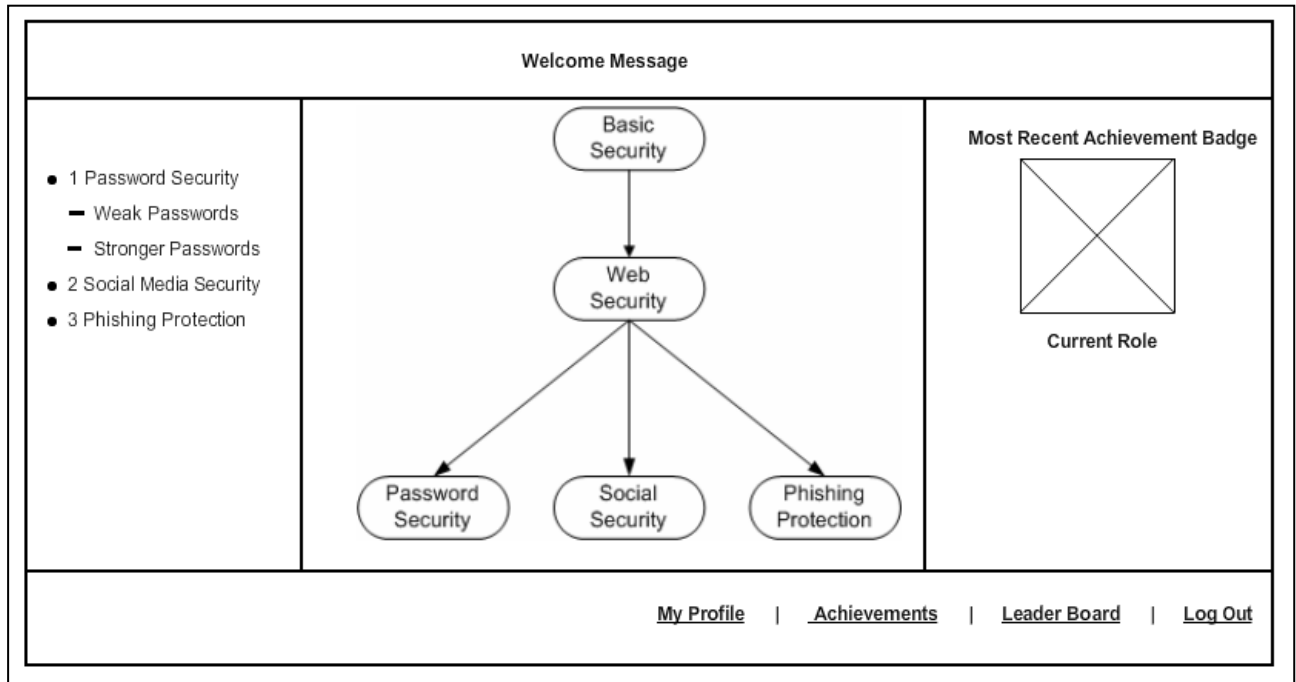
**Figure 6-13: High-level Design of Game (Source: Own)**

The game component initiates when the user logs into the game. With a successful login the user would be presented with the “Topic Tree”. This page would provide the user with the gaming topics and performance indicators. The use of badges provides a visual presentation of the performance indicators. The user can navigate to the topics, which provide access to learning material, as well as an assessment feature. In addition, access to the leaderboard and profile information is presented. The leaderboard not only indicates the user’s performance and progress, but also compares progress with other users playing the game. The user also has the option to log out of the system at any time during the play; the state of the game is stored after every interaction with the gaming platform.

The objectives of the gaming platform are to ensure users become aware of threats originating from the use of computers, and to transfer knowledge that allows the user to understand and mitigate these threats with the knowledge acquired from the information security awareness game. As described in Section 6.2.2.5, the richness of the information has an impact on the effectiveness of knowledge transfer and understanding - the use of hypertext and multimedia is ideal for this gaming component. Therefore, the topics section

presents the information resources used to transfer knowledge in the game, in the format of slides and videos.

Screenshots are used to explain the flow of the different components of the game. The user will be directed to the selected topic and provided with an interface (See Figure 6-14).



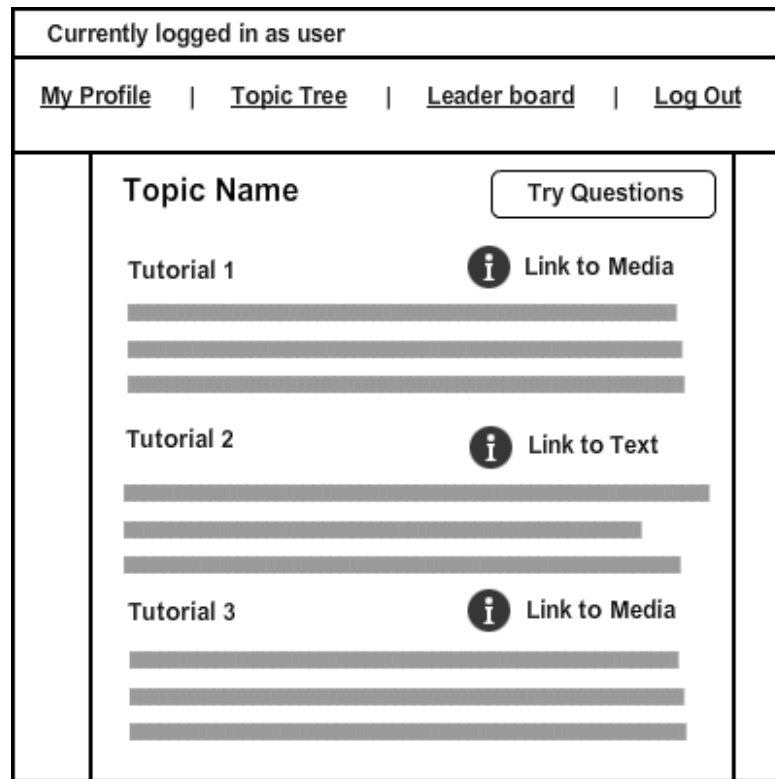
**Figure 6-14: High Level View of Game Prototype (Source: Own)**

The layering of subject matter as described by Khan et al. (2011) addresses the requirement of using a weighted method to incorporate the difficulty of content. Each level represents a more complex level of topics.

In order for the user to progress to more advanced topics, a user is required to 'unlock' the next level. To do so, users need to answer ten consecutive questions correctly on the preceding level. Questions are chosen at random from the pool of compiled questions for each level. The questions are also created from a practical point of view. This ensures the knowledge assessed replicates the real world and the user can apply it when the scenario is encountered. The layout presents a visual path that the user needs to complete on the selected topic. The path also represents a structure of progress to show the advancement in difficulty. In other words, the difficulty increases as the user progresses through each layer.

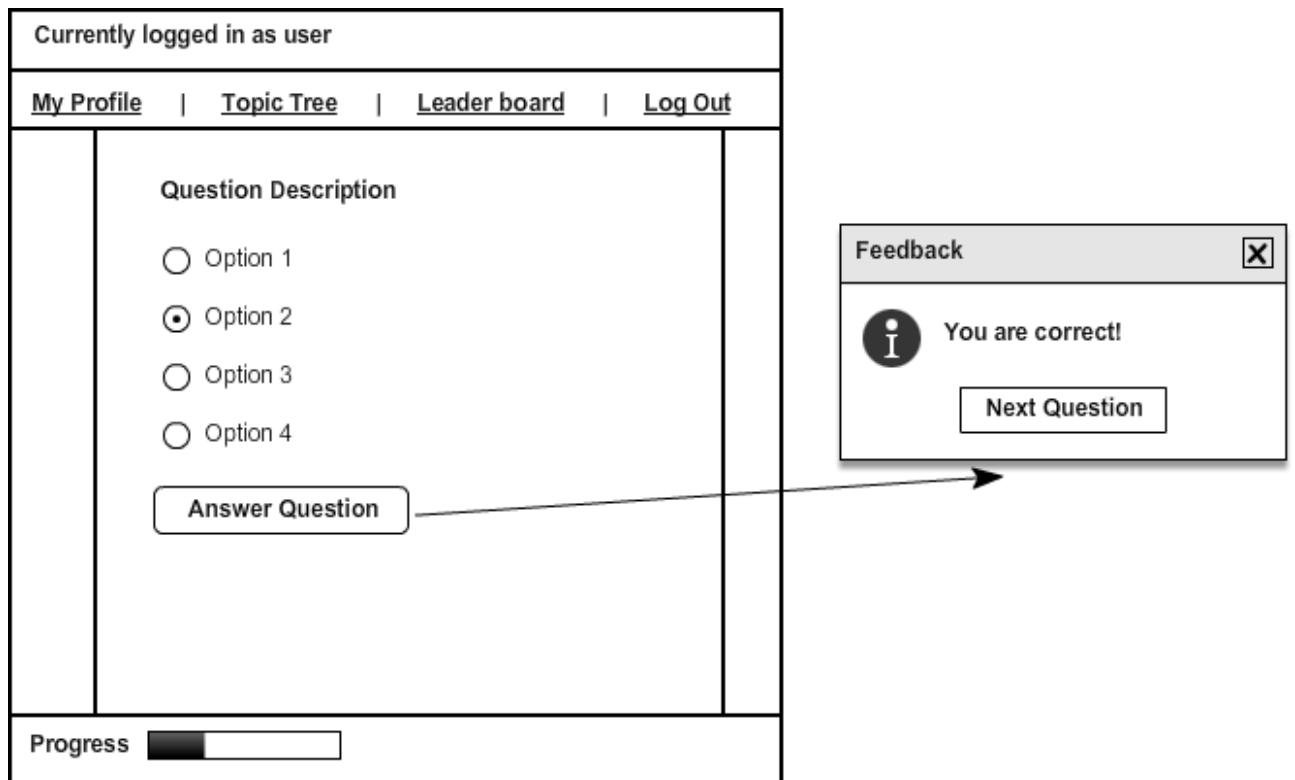
The user can access the quiz or tutorial component by selecting a section within the topic breakdown. The tutorial component contains information on the topic and is represented

by slides or videos, which ensure the user not only becomes aware of the subject matter, but also understands it (Figure 6-15).



**Figure 6-15: Mixture of Hypertext and Hypermedia (Source: Own)**

In the case of the quiz, the user can assess the knowledge on the topic and subsequently progress in the game and obtain points to compete with other users. The quiz consists of multiple choice questions and is randomly selected from the pool of questions created on the topics (Figure 6-16). As described earlier, the questions have weights assigned to them indicating the difficulty level. The use of the progress bar provides the user with a visual indication on progress within the quiz as prescribed by Nielsen (2005).



**Figure 6-16: Sample Question and Status (Source: Own)**

Other factors were taken into consideration to ensure the game is easy to use and intuitive, while providing the user with information on how to proceed and recover from errors without affecting the game. For example, if the game only made use of links, the user would only have with one method to play the game.

Badges were also implemented. This helped to indicate achievements for the users. The badge and achievement system encourages users to try and attain better scores and complete more sections. Different badges indicate different achievements, and the system automatically creates notifications to inform all users about the progress and achievements of other users. For example, a badge can be awarded to a user who answers ten questions correctly, or another badge can be awarded if a user accesses the game in three consecutive days (Figure 6-17).

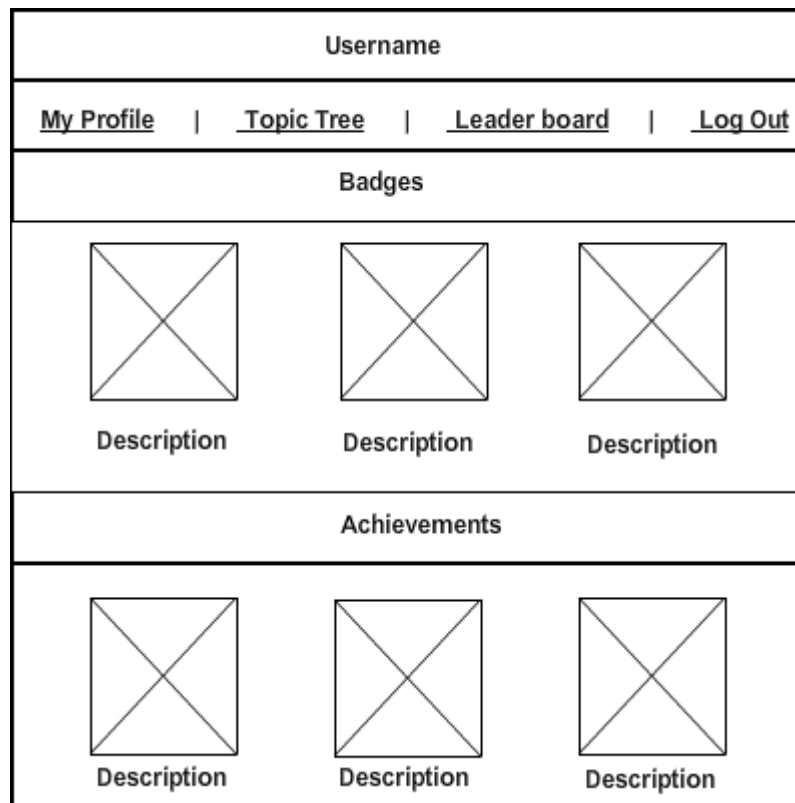


Figure 6-17: Badges and Achievements (Source: Own)

By using a social networking application to run the game, users can view their friends' activities, and this would also encourage repeated use. Social networking sites provide application programmable interfaces to encourage developers to develop and deploy games within the social networking site environment. In this way, by placing the game in a popular medium such as a social networking site, the appeal of the game is strengthened and this also promotes user acceptance. Overall, the game has been designed taking into consideration the various requirements prescribed by the literature.

## 6.4 Conclusion

This chapter addressed the development phase of the NIST information security awareness framework by identifying a platform to deliver the information security awareness program to the intended participants. Section 6.2 proposed the use of an autonomous system, which could conduct an information security awareness program and measure the information security awareness levels of participants without human intervention. The system consisted of several components which could operate individually, but could also be combined to achieve the objective of autonomous

information security awareness programs. The system requirements and design considerations were discussed.

Section 6.3 shifted focus to one of the components of the autonomous system. The Awareness Collection component not only collected data but also engaged with users through the use of game play. Many information security awareness programs use posters, informal and formal training, but these do not have the components to promote learning that game play has.

Initial research has shown several games were designed and developed to promote positive behaviour change. The use of gaming concepts provided metrics to calculate the effectiveness of the knowledge transferred as seen by CyberProtect and CyberSiege. In other words, the actions taken in the games demonstrated a clear understanding of concepts and application of it within a situation. This study builds on the concept of gaming to transfer knowledge to the participants. It should be noted different types of games exist which include interactive, text based and turn based. Each of these types has a design consideration as they are developed in different ways but have the same underlying objective. The type of game would be selected based on the method used to collect data from the participants (Section 7.2).

Section 6.3.2 investigated the design requirements for using game play to delivering information security awareness programs. The design considerations were then used to develop a prototype gaming component (Section 6.3.3).

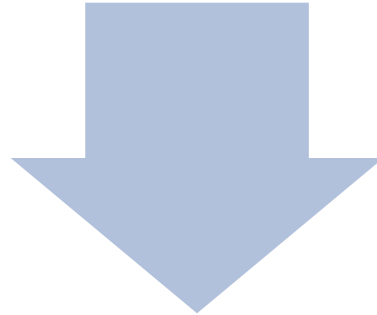
The resulting design considerations identified in this chapter, together with the prototype feedback, were implemented in the development and deployment of a social networking game discussed in the next chapter.

The first phase of the NIST framework identified the need and topics required for the information security awareness program (Chapter 5). The second phase of the NIST information security awareness framework, which focused on the delivery platform required to transfer the knowledge on the selected topics, was discussed in this chapter.

The next phase of the NIST information security awareness framework, which focuses on the implementation of the information security awareness program, is described in the next chapter. Data collected during the information security awareness program would be analysed to determine the effectiveness of incorporating games in information security awareness programs.

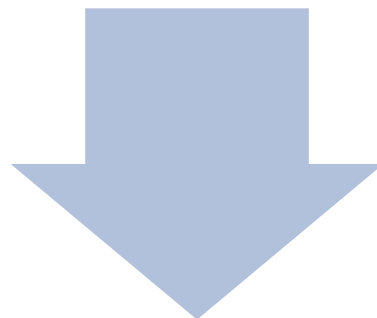
## Chapter 7: Implementation (Data Collection)

Chapter 6 - Development (Distribution Platform)



## Chapter 7 - Implementation (Data Collection)

- 7.1 Introduction
- 7.2 Research Design
- 7.3 Methodology
- 7.4 Limitations
- 7.5 Ethical Consideration
- 7.6 Conclusion



Chapter 8 - Post Implementation (Analysis of Data)

Figure 7-1: Layout of Chapter 7

## 7.1 Introduction

The main aim of the study was to determine whether game play is an effective component within an information security awareness program. The previous chapter addressed the development phase of the NIST information security awareness framework. The next phase in the NIST framework discusses the implementation of the information security awareness program and is described along with the data collection process used in this study. The analysis of the collected data would subsequently support the argument that the learning effect can be enhanced with the use of online games. In addition, the findings from the analysed data could be used to improve future information security awareness programs.

The first section of this chapter addresses the selection of the data collection technique to be used (Section 7.2); this is followed by an in-depth description of the research instrument that implements the selected data collection technique (Section 7.3). It is important to have a clear understanding of the limitations of the method used, and these are described in Section 7.4. Ethical procedures are addressed in Section 7.5 to ensure that the study is aligned with the university's ethical guidelines.

## 7.2 Research Design

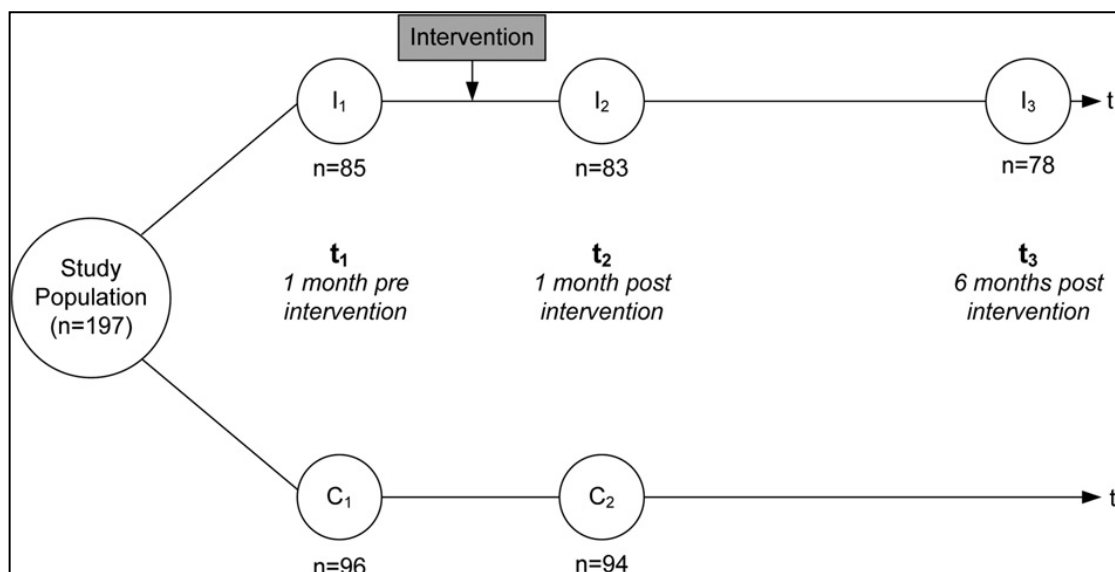
This section describes the research tool used during the data collection. Research conducted within the information security awareness domain is reviewed in the pursuit of selecting the most appropriate research tool. It also highlights the different research tools used within the domain of information security awareness. The following work was reviewed to select the best suited research tool:

- In 2009, Szewczyk and Furnell (2009) assessed the online information security awareness of Australian Internet users using open ended interviews. The interview process was attended and completed by twenty-three participants. They were recruited by personal invitation or by friends. Each interview lasted 60 minutes and the gender distribution was mostly male.
- Fung, Khera, Depickere, Tantatsanawong and Boonbrahm (2008) reported on a pilot study for raising information security awareness amongst students in Thailand. The study utilised a simulation game called CyberCiege (2004). The experiment involved two groups of eight students each. Each group first completed pre-test questions. Next, one group played the game while the other attended a short



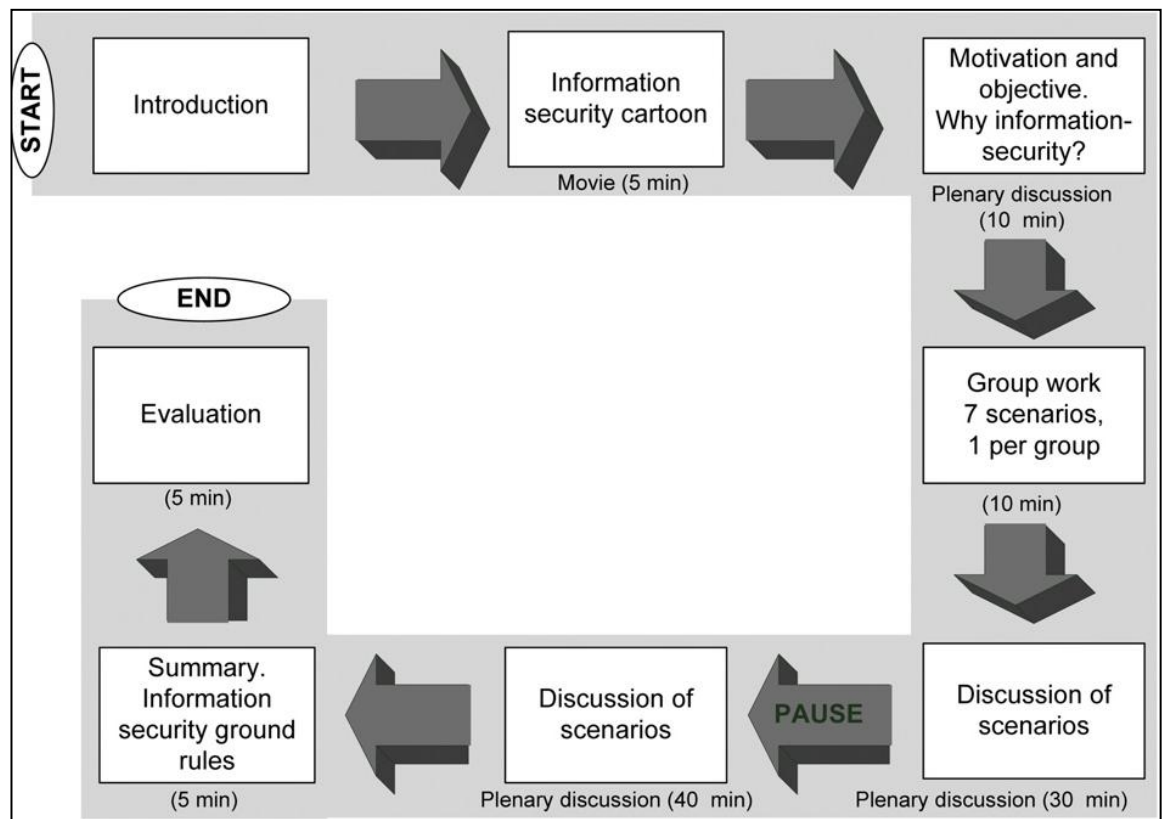
training session. The group playing the game had one week to complete the game, and then answered post-test questions. The other group attended a 60 minute training session, which included a 10 minute session to raise any questions. This allowed the students to clarify any awareness content that was not understood and was followed by post-test questions.

- Stanton, Stama, Mastrangelo and Jolton (2005) used both interviews and surveys to analyse the security behaviours of end users. They created a taxonomy of security behaviours by interviewing information technology professionals, managers and regular employees. A survey was created using the taxonomy and then randomly distributed by postal mail.
- The work conducted by Albrechtsen and Hovden (2010) evaluated the effectiveness of an information security awareness programme with the use of an intervention study. They used a quantitative survey and a qualitative approach that combined interviews, group conversations and observations of the intervention as methods to collect data. Surveys were used before and after the intervention to evaluate if any intended changes occurred. The web based surveys were sent via email to the participants. Two groups were used for the study: an intervention group denoted by “I” with 85 participants initially and a control group of 96 participants indicated by “C”. Figure 7-2 shows when the intervention was scheduled.



**Figure 7-2: Time-Series Research Design with an Intervention Group and a Control Group (Albrechtsen & Hovden 2010)**

The process for the intervention is illustrated in Figure 7-3.



**Figure 7-3: Content and Processes of an Information Security Workshop (Albrechtsen & Hovden 2010)**

- Rezgui and Marks (2008) conducted an exploratory study on information security awareness in higher educational institutions in the United Arab Emirates (UAE). The researchers combined quantitative (questionnaires) and qualitative (interviews, documentation and observations) methods to collect data which allowed them to obtain an accurate view of the participants' level of information security awareness. The data was collected from July 2006 up to and including September 2007.
- Shaw et al. (2009) determined the effectiveness of information richness on information security training. A sample of 240 students from Taiwan was used for the study. A pre-test was used to ensure that all the participants had the same information security awareness levels. Course material concerning the selected information security awareness topics were provided to the students. Next, a post-test assessment was provided to each student. This was followed by the students' participation in an experimental system to record the learning behaviour of the student.
- Dodge, Carver and Ferguson (2007) used security exercises to educate users about phishing attacks. This was achieved by developing a prototype system which

conducted phishing attacks, resulting in the identification of users who were susceptible to phishing attacks.

- Kruger and Kearney (2006) developed a prototype for assessing information security awareness within an international mining company. Their tool employed techniques from the social psychology field, which identified affect, behaviour and cognition as three components. They used thirty-five questions to test knowledge, attitude and behaviour from the respondents, who were located at different company sites throughout the world. In addition, they emphasised that the development of a measuring tool needs to address the following challenges:
  - What to measure?
  - How to measure it?
- Chou and Peng (2011) evaluated the Teachers Awareness of Internet Safety (TAIS) project over a ten year period in Taiwan. The project consisted of three phases. The first phase (2000 – 2002) aimed to build an online learning website. The data was collected using surveys and interviews which were completed by the teachers. The second phase (2003 – 2006) focused on improving the training programmes developed in the first phase. Surveys and interviews were again used to collect the data. The last phase (2007 – 2009) continued with the development of the online learning website and teacher training programs. Once again data were collected using surveys, interviews and evaluations.

All the different research designs utilised in the work described above are summarised in Table 7-1. It clearly indicates that surveys, questionnaires and interviews are the most popular research tools used for collecting reliable data in the information security awareness domain. These research designs will now be discussed in detail to understand the advantages and disadvantages of each method of data collection.

**Table 7-1: List of Information Security Awareness Data Collection Used**

Study	Surveys / Questionnaires	Interviews	Documentations	Observations	Evaluation	Group Conversations
Szewczyk and Furnell (2009)		X				
Fung et al. (2008)	X					
Stanton et al. (2005)	X	X				
Albrechtsen and Hovden (2010)	X	X		X		X
Rezgui and Marks (2008)	X	X	X	X		
Shaw et al. (2009)	X			X		
Dodge (2007)	X			X		
Kruger and Kearney (2006)	X					
Chou and Peng (2011)	X	X			X	

### 7.2.1 Interviews

The interview method has several advantages, including having a higher response rate than surveys distributed to respondents. The presence of the interviewer can increase responses; for example, the participant can ask the interviewer to clarify a question. Another advantage is the observation of the respondent's behaviour, which is not possible when surveys are used. These advantages were also suited for this study as the clarification of questions and observation of the participants was possible during the data collection process. The disadvantages of using interviews are possible the lack of interviewing skills, cost and time (Opdenakker 2006). The interviewer requires experience on methods to lead the participants using questions to obtain the required information. Also, the time necessary to collect the data using interviews was not suitable for this study. In other words, the collection of data through interviews would not have made it feasible as interviewing a large number of participants would be time consuming. Furthermore, to interview each student after the training session would require more than one interviewer to ensure that the data is collected within one day, thus increasing the cost, as well as introducing the bias of each interviewer, which could also impact on the validity of the results. Interviews, based on the reasons discussed, were not considered for use in this study.

### 7.2.2 Surveys and Questionnaires

McDonald and Adam (2003) conducted a study to compare online and postal surveys as methods to collect data. The results of their study indicated that online data collection is more cost effective and provides a platform for faster data collection. Questionnaires, which form part of the associated survey data collection techniques, would be used for this study (Pfleeger & Kitchenham 2001).

It was important to understand the weaknesses of questionnaires as a collection method technique for this study. Evans and Mathur (2005) identified the following weaknesses attributed to using online surveys:

- Perception as junk mail
- Skewed attributes of Internet population
- Questions about sample selection and implementation
- Respondent lack of online experience
- Technology variations
- Unclear answering instructions
- Impersonal
- Privacy issues
- Low response rate

As questionnaires are a subset of surveys, the weaknesses associated with surveys would also affect questionnaires. The way in which this study addresses these weaknesses are discussed next.

Junk mail is usually sent by marketers to advertise products or services, but has little value to the recipient of the mail, since the mail is sent to random recipients. During the data collection process of the study, the links to each questionnaire are provided in person to the participants. No emails containing links to the questionnaires are sent to the participants, which resolved the potential weakness that the participant might identify the survey as junk mail.

The weakness of not having a true representation of the general population is addressed by pre-selection of participants. They are selected from a student group attending a tertiary institution, and are classified as information security novices. Thus, the participants have received no formal computer security or information security awareness training. This

addresses the weakness of skewed attributes among the general Internet population and also resolves the issue of the sample selection.

Another concern of sample selection and implementation relates to sending online services to any person on an email list who is willing to complete the questionnaire. Another example is that of a company sending a questionnaire about technical content to non-technical respondents. In other words, the respondents might not be the target participants.

The distribution of the questionnaires in this study is controlled and the respondents meet the required criteria which include: young age group (between 17 and 23 years old), attending the information security awareness training, and not having a cybersecurity background. The weakness of lacking online experience was addressed by using a controlled environment for the respondents with the presence of the researcher during data collection.

Each session started by explaining the entire process and providing assistance to the respondents who required help to complete the questionnaire. This included the distribution of unique numbers to be used by the respondents as a unique identifier for each session. In addition, technical assistance was provided to ensure the computers were fully functional and could be used by the respondents.

The technology variation weakness was overcome by having all the respondents located in the same venue, which guaranteed all the computers and network connections had the same performance during the data collection period. It should be noted that a network failure could mean that the respondents would not be able to access the questionnaires; however this was addressed by having hard copies of each questionnaire available. This ensured that the data could be collected even in the event of a network failure.

Unclear instructions can easily hamper the progress and quality of the data collection as the respondent might not understand how to answer the questions. The interpretation of questions depends on the knowledge and understanding of the respondent who is answering the question; not all respondents have the same background. The weakness of unclear instructions is mitigated by the presence of the researcher during the data collection. All unclear instructions could be addressed immediately, ensuring that respondents had a clear understanding of the questions in the questionnaires.

The weakness of the impersonal effect, which implies the questionnaire is administered without human contact, was addressed by the presence of the researcher in the same venue as the respondents. Although the questionnaire was administered using technology, the human element was present to address any questions and personalise the process.

The weaknesses of privacy and security issues are important concerns for the respondents. These were addressed as follows: the web application used to collect the data used a secure connection, which encrypted the data on the network and prevented automatic access to the data in the event of data interception. Furthermore, each respondent was provided with a unique identifying number to complete the questionnaires, and no personal data was captured during the collection process. The unique numbers are used to link each respondent to a completed questionnaire, but still maintain anonymity.

A list is created where each person is provided with three unique numbers used for each questionnaire. An example showing numbers for three respondents is given in Table 7-2. A complete list for all the respondents used during the data collection can be found in Appendix E.

**Table 7-2: Example of List with Unique Numbers**

<b>Name</b>	<b>Number 1</b>	<b>Number 2</b>	<b>Number 3</b>
Person 1	KXV3IFA	S2GCEKD	YC7GM3A
Person 2	YLVZ9JB	HIJ4MCA	XZ5IWJC
Person 3	ZBV6PNB	UQY4Y7B	2BFB9JB

To explain further, a respondent was assigned a name in the beginning of the collection process. “Person 1” will sit at a computer during the pre-assessment and the unique number, KXV3IFA, will be assigned for this particular questionnaire. When the respondent, “Person 1”, is ready to complete the first post assessment, then the number, S2GCEKD, is provided for completing the first post-assessment questionnaire. The respondent is still sitting at the same computer. Finally the number, YC7GM3A, is provided when the respondent, “Person 1”, is ready to complete the last post assessment. No personal information is captured to link the respondent to the unique identifier “Person 1”.

The last weakness of having a low response rate was also addressed by having the respondents in the same venue during the data collection. The respondents were made aware that the entire data collection consists of different phases, as described in Section 7.3.1.2, and the questionnaires formed part of three of the five phases.

All the identified weaknesses when using online questionnaires were addressed during the data collection process. The use of online questionnaires was selected as the data collection method for this study because of the cost effectiveness and the speed at which the data could be collected and analysed.

## **7.3 Methodology**

The implementation of the research instrument, the data collected and the analysis of the collected data are discussed next.

### **7.3.1 Research Instruments**

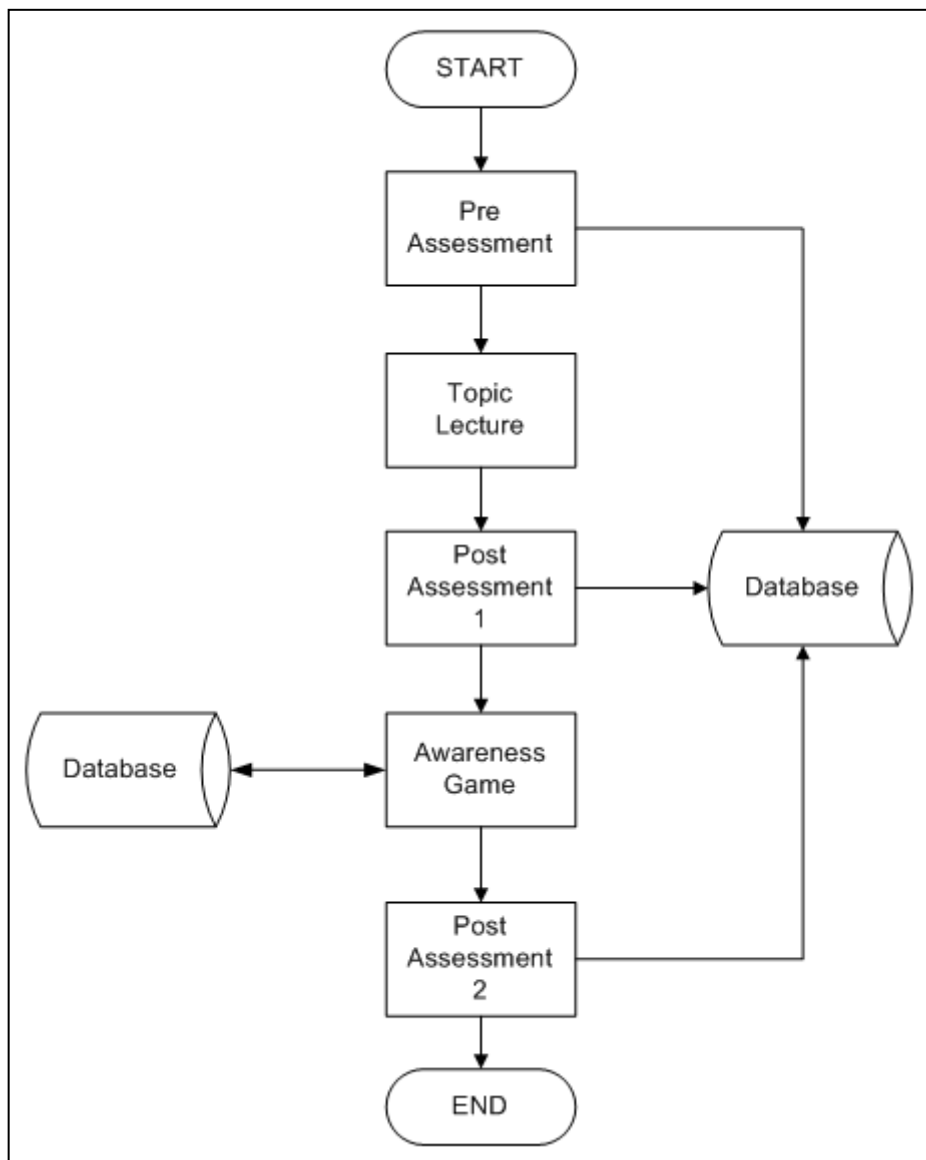
This section outlines the method used to collect the data required to determine the effectiveness of game play as part of an information security awareness program. The process used during the data collection is discussed first. This is followed by the description of the schedule implemented for the data collection. Finally the two platforms used for the data collection are described.

#### **7.3.1.1 Data Collection Process**

The data collection process included different components to capture data from the participating respondents. The data collection process started with the respondents completing a pre-assessment questionnaire. The objective of the pre-assessment questionnaire was to determine the current information security awareness levels of the respondents (See Appendix B). This also formed the baseline against which the subsequent questionnaire results will be compared to determine the effectiveness of the different knowledge transfer methods.

The transfer of information security awareness knowledge was done through a training session and a computerised game play session. The training session consists of a lecture where all the topics were presented to the respondents once the pre-assessment questionnaire had been completed. Figure 7-4 summarises the steps followed during data collection.





**Figure 7-4: Data Collection Process (Source: Own)**

The first post-assessment questionnaire was administered after the training session (See Appendix C). The data collected were compared to the pre-assessment results to determine if any knowledge had been gained and retained. Next, the respondents participated in a social networking site game. The game focused on the identified information security awareness topics and used game play components to enhance the learning experience.

Rovee-Collier, Evancion and Earley (1995) studied the effects of repeated study sessions and coined the term “spacing effect”. The “spacing effect” is the degradation of knowledge over a period of time. In other words, knowledge recall will decrease as time elapses. The time window is the limited period during which the same knowledge can be exposed to the

person for the second time before the knowledge is forgotten from the first exposure. The more the same content is learned, the longer it will take before the knowledge is forgotten. The “spacing effect” is depicted in Figure 7-5.

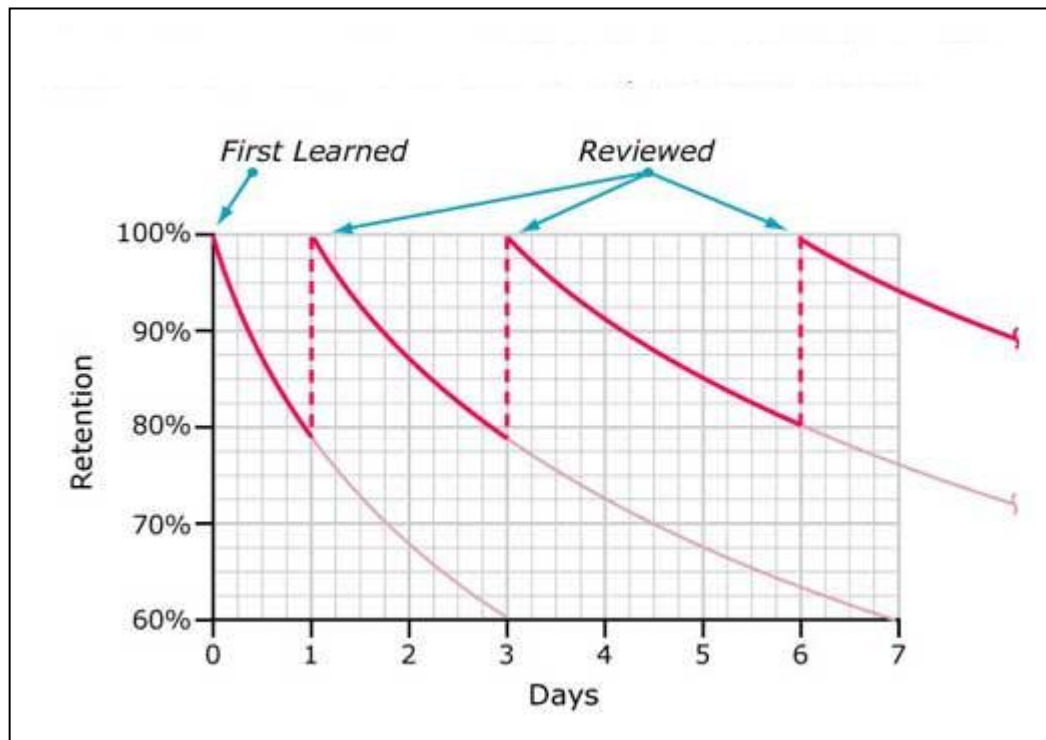


Figure 7-5: Spacing Effect (De la Rouviere 2012)

Bell, Harless, Higa and Mangione (2008) also conducted an experiment to determine the retention of knowledge over a period of time. Their findings supported the notion of reinforcing newly learned knowledge to optimise retention. These findings are used as part of the design of this research. In other words, the participants will be exposed to new knowledge more than once to improve their retention rate.

A second post-assessment questionnaire was completed by the respondents once the game had been completed (Appendix D). The data collected here was to be compared to the pre-assessment and the first-post assessment questionnaire to determine the effectiveness of game play as a mechanism to enhance learning.

### 7.3.1.2 Survey Schedule

Three questionnaires were used during the data collection phase. The administration by the research team of each questionnaire took place at predefined stages during the collection of the data from the respondents. Each questionnaire consists of 35 questions which cover the seven identified information security awareness topics (See Appendix B,

Appendix C and Appendix D). This indicates that each topic in a questionnaire has five questions.

In addition, the focus of each question is captured across all three questionnaires. For example, it is important for the respondent to understand how to identify a weak password. Three questions were created to address the requirement of identification of a weak password. These three questions were distributed across the three questionnaires. The respondents were exposed to a question addressing the identification of a weak password, in each questionnaire.

The questionnaire schedule is tabulated in Table 7-3 and a detailed description follows. The pre-assessment was designed to determine the initial information security awareness level of a respondent. The time allocation allows the respondent sufficient time to complete the questionnaire. The respondent is allowed one minute to answer each question. An additional five minutes have been allocated to each questionnaire; this was done to take into consideration the time used when the respondent submits the answers for each section in the online questionnaire. Not all networks have the same network speed, which implies that all the respondents may not complete the questionnaires in the same time. The first post-assessment was designed to determine if any knowledge had been retained after the training session. The results from the first post-assessment are compared with the results of the pre-assessment, which should give an indication of whether the training session has transferred any new knowledge to the participants. The second post-assessment objective is to help identify the effects from the game play on the retention of knowledge. The resulting data is compared to the first post-assessment results, and should indicate a positive correlation, suggesting that adding game play as part of an information security awareness program does improve learning and the retention of knowledge.

**Table 7-3: Survey Schedule**

Order	Item	Type	Time
1	Pre-Assessment	Questionnaire	40 min
2	Information Security Awareness Training		180 min
3	Post-Assessment (1)	Questionnaire	40 min
4	Game play		120 – 180 min
5	Post-Assessment (2)	Questionnaire	40 min

### 7.3.1.3 Questionnaire Topics

The selection of the information security awareness topics is discussed next. The NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, details the steps required to create an effective awareness program (2003). The first step focuses on the design of the awareness program, which requires the performance of a need analysis to understand what security topics need to be addressed by the information security awareness program. The identification of the topics required for this study was discussed in Chapter 5.

Table 7-4 lists the information security awareness topics as previously identified in this research. These topics include malware, social networking sites, phishing, spam, web browsers, passwords and cyberbullying. The training content of each of these topics addresses the threats identified. The design of the questionnaire and the social networking game also focuses on these topics to ensure alignment with the required objective of the information security awareness program.

**Table 7-4: Information Security Awareness Topics**

Number	Topic	Total Number of Questions per Topic (Pre-Assessment)	Total Number of Questions per Topic (Post-Assessment 1)	Total Number of Questions per Topic (Post-Assessment 2)
1	Malware	5	5	5
2	Social Networking Sites	5	5	5
3	Phishing	5	5	5
4	Spam	5	5	5
5	Web Browsers	5	5	5
6	Passwords	5	5	5
7	Cyberbullying	5	5	5
<b>Total</b>		<b>35</b>	<b>35</b>	<b>35</b>

### 7.3.1.4 Online Survey

The three questionnaires were administered from the SurveyShare website, which is an online tool for the creation of surveys. For this study, questionnaires were created from the template provided by the SurveyShare platform. Each of the questionnaires had a unique Uniform Resource Locator (URL) assigned to them. This ensured that the participants could only access the questions associated with the questionnaire. Some of the questions in each questionnaire contain images: the participants had to answer the question according to the content depicted in the image (See Figure 7-6 for an example).



Figure 7-6: Example of Online Questionnaire Questions (Source: Own)

SurveyShare has a reporting feature which provides easy access to the analysed data captured by each questionnaire. Using the online medium has a few advantages over the

use of paper: the surveys can be accessed from any location and the processing of each survey is almost immediate. The collection of the data from the participating groups together with the reporting was completed within a day. Printed copies of the surveys were created to use in the event of loss of network connectivity or the unavailability of the SurveyShare website. A loss of network connectivity would also mean that the game play would not be possible since the game is hosted within Facebook, a social networking site.

#### **7.3.1.5 Social Networking Site Game Play**

The concept of game play was incorporated into the information security awareness program by using social networking sites as the platform. Facebook has many successful games using their platform, for example, Farmville and Mafia Wars. In addition, many users are familiar with Facebook and have established a trust relationship with the platform. Users can access the game from the already existent platform. The participants in the research required a Facebook account to access the game. The game is developed around a questionnaire which focuses on the identified information security awareness topics. Game play features are incorporated around the questionnaire to create a competitive environment. These features include:

- **Achievement badges** - These provide a visual status to the user about achievements obtained during the game and included the 'leader', 'on-a-roll' and 'busy bee' badges (Figure 7-7). The 'busy bee' badge is assigned to a user who accesses the game on two consecutive days. The 'on-a-roll' badge indicates the user has answered three consecutive questions correctly. To keep this badge the user needs to continue answering questions correctly. The 'leader' badge indicates that the user is the current leader of the game. The timeline will be immediately updated when a user obtains this badge. It should be noted that the proposed prototype discussed in Section 6.3 used three days as the metric to determine when to assign the badge. As the information security awareness program was only conducted on a single day, this badge was not presented to the users who played the game.

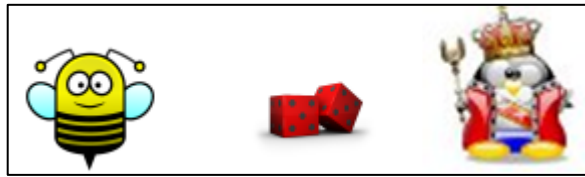


Figure 7-7: Achievement Badges (Source: Own)

- **Leaderboard** - Lets users see who is currently leading in the game. The points acquired by the user are also displayed to indicate to other users how far ahead the leader is. This helps to promote competitive behaviour.
- **Timeline** - Provides a real-time feed on the activities of each participant. The timeline is updated once the participant answers a question, obtains an achievement or becomes the leader. No negative feedback is displayed in the timeline. Positive behaviour is acknowledged and promoted with the use of the timeline.
- **Progression** - Displays the participant's progression through the game. The progress bar indicates how many questions have been answered.
- **Performance** - Displays the participant's performance over a time period. Every correct answer adds points to the overall performance score. When the participant answers incorrectly, points are deducted. For example: the participant answers a question correctly and earns performance point; when the participant answers another question correctly, the total performance points will be increased, and the graph will clearly show a positive upturn; however, three incorrect answers will indicate a negative downturn.
- **Feedback** - Allows the participant to understand what the correct answer to the question was in the event of an incorrect answer. Displaying the reasoning of the correct answer provides the participant with additional learning opportunity.
- **Points** - A point system is used to determine who is the leader and also promotes competition amongst the participants. Every correct answer obtains 100 points. The leader gets double points when answering questions correctly. For example, the leader would get 200 points when a correct answer is provided.
- **Inventory** - The inventory contains a list of items that can be bought with points obtained within the game to provide protection against game events that randomly occurs during play. These are discussed in Section 7.3.2. The inventory items are illustrated in Figure 7-8 and are described as follows:

- **Anti-Virus** - This item protects the user against a virus infection event.
- **Password Training** - This item is used to protect the user against an account hacking event.
- **Firewall** - The firewall item provides protective measures against a worm infection event.
- **Social Networking Site Safety Training** - This item protects the user against a cyberbully attack.
- **.Backup Harddrive** - The backup harddrive item provides protection against a hard drive crash event.



**Figure 7-8: Inventory Items (Source: Own)**

The game is developed in Hypertext Preprocessor (PHP) and is deployed within Facebook. The game uses an Application Programming Interface (API), which allows developers to create applications which can be deployed within Facebook. An additional benefit of using the Facebook API is the accessibility to Facebook specific features, which include access to the Wall or Facebook timeline of the user, the authentication mechanisms and integration into Facebook.

Participants can log into the social networking site Facebook and access the game. A question and corresponding answer options are displayed to the participant. The participant selects an answer and submits a response. The user is immediately informed if the answer is correct. If not, feedback which contains the reasoning for the correct answer is provided to the user before the next question is displayed.

A database with 142 questions covering all the information security awareness topics identified has been created. The game uses the questions from the database. The questions are randomly selected by the game and displayed to the participant. All the different features are updated after the submission of an answer. This process continues until all the questions have been answered.

An example of the user interface is depicted in Figure 7-9.



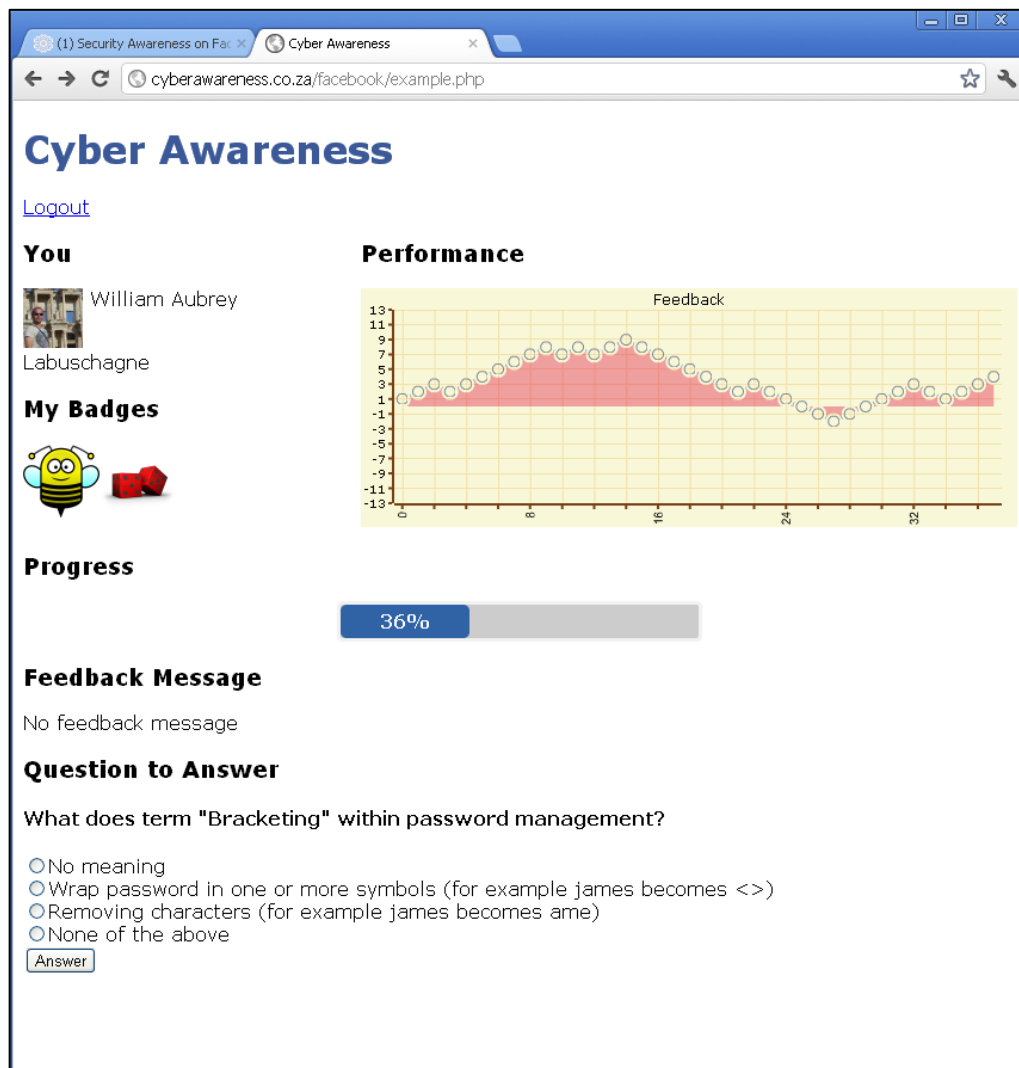


Figure 7-9: CyberAwareness Social Networking Site Game (Source: Own)

### 7.3.2 Game Events

This section describes the different game events that can occur during game play. A random number is generated during the play of the game; an event is generated when this random number falls in between specified ranges (Table 7-5). The triggered event is displayed to the user and affects the user's score, if the user does not have the corresponding item in the inventory list. Items in the inventory list can be obtained through the accumulation of points and points are earned by answering questions correctly.

For example, if the game event triggered is a virus infection then the user needs to have the anti-virus item to avoid losing points. Otherwise, 500 points will be deducted. The user can obtain these items through the accumulation of points by answering questions correctly. If enough points have been acquired during the play of the game, then the user

can use these points to obtain available items. For example, the user needs to accumulate 1000 points to obtain the “Password Training” item.

**Table 7-5: Game Events**

Value Ranges	Event	Point Effected	Item	Points Used to Acquire Item
100 - 1000	Virus Infection	500	Anti-Virus	500
1001 - 15999	No Event			
16000 - 23000	Worm Infection	750	Firewall	600
23001 - 29999	No Event			
30000 - 39000	Cyberbully Attack on Social Networking Site	1000	Social Networking Site Safety Training	750
39001 - 44999	No Event			
45000 - 60000	Facebook account hacked due to weak password	1500	Password Training	1000
60001 - 89999	No Event			
90000 - 120000	Data loss due to harddrive crash	2000	Backup Harddrive	1500

### 7.3.3 Data

The previous section described the methods implemented to capture data from the participants. This section describes the data gathered during the collection process. The participants were undergraduate students from the University of Venda (South Africa) who are registered for a degree programme in Computer Science and Information Systems. The students who graduate from the course will have sufficient knowledge, skills and competence to conduct development work within the information systems business sector. The layout of the course addresses many aspects of information systems which include Introduction to Computer Systems, Database Fundamentals, Data Communication and Computer Networks, Software Engineering and Artificial Intelligence (University of Venda 2013). However, no module within the course addresses security within information systems or networking. This implies that the participants will not have been exposed to the wide variety of security-related topics covered by the information security awareness program.

In spite of the lack of security-related modules, some of the participants could have directly or indirectly learned about some of the information security topics. To elaborate, the use of privacy controls on social networking sites might have been emphasised by security-

related events propagated by various news sources. For example, the social networking site Facebook had to compensate some users after their privacy was violated (Miller 2013). In this way the participant could have indirectly learned about the use of privacy controls to manage private information. Another example of indirect learning would be the creation of strong passwords; many websites provide users with feedback to enforce the use of strong passwords.

In direct learning, the participant chooses to learn about security-related topics. For example, the participant could have an interest in computer security and learned about the different aspects from websites that focus on security-related topics like Net-Security (<http://www.net-security.org/>), Hackin9 (<http://hakin9.org/>) and Security Magazine (<http://www.securitymagazine.com/>). In addition, the students that form part of the sample have formal education course outcomes which are aligned with most of the tertiary institutions within the Gauteng province in South Africa. The Tshwane University of Technology (TUT) only provides an information security module during the fourth year of studies. The University of Pretoria (UP) also addresses information security during the latter part of the studies. The undergraduate degree at University of Johannesburg (UJ) does not contain a computer security module, but offers certificate courses that focus on cybersecurity from the first year of study. Furthermore, the University of South Africa (UNISA) includes computer security as part of postgraduate studies. The participants from the University of Venda were selected due to their availability to partake in the study as well as their opportunity to transfer knowledge to other rural communities.

During the literature review, it was shown that quantitative and qualitative data could be used for information security awareness research. Dey (2003) described qualitative data as a measure of relative worth based on the evaluation from a general observer, for example, how a person emotionally experiences a movie or book. In other words, data that can be observed but not measured. The most common method is the qualitative research interview, but other forms of the data collection can also include group discussions, observation and reflection field notes, various texts, pictures, and other materials (Major & Savin-Baden 2013). Qualitative data was not included in this study because limited resources were available to complete the study. The use of interviews, group dialogue and reflection would have provided more data in conjunction with the quantitative data to form an accurate conclusion.

Quantitative data is measurable data, for example the height of people, colour of hair, and number of correct answers. The most common method used in quantitative research is the use of surveys or quizzes (Balnaves & Caputi 2001). The use of surveys and quizzes to determine the awareness levels of a target group has been considered in Section 7.2 and is listed in Table 7-1. This study used quantitative data with the limited resources available and it was anticipated that this would provide enough evidence to prove gaming to be effective to reinforce learning.

Quantitative data was captured from two sources; the surveys which served as quizzes to measure the knowledge levels and the online game to track the progress of the participant and reinforce the learning process. The data collected from these two sources are described in the following two sections.

#### **7.3.3.1 Surveys**

Online surveys were used to collect data from participants in the form of quizzes. The questions were displayed to the participant together with possible answers. Only one of the possible answers presented to the participant was correct, while all the other answers were incorrect. The quantitative format allowed the analysis of the data to be conducted with the use of Microsoft Excel (Dretzke 2005) and R (R Core Team 2013). R is a free statistical analysis language while Excel forms part of Microsoft Office. Both these software packages not only provide powerful statistical analysis capabilities but also graphing of results.

The online survey web application stored the answers in a database and allowed the researchers to export the data into different formats including comma separated values (CSV) and Microsoft Excel spreadsheets. This allows the data to be imported into other software analysis tools. The answers resemble the option selected as the most viable option from the available list by the participant. The answer is depicted by an integer number that corresponds to the option: for example, the third option would be represented by a "3". The questions were also categorised to resemble the different topics. The answers provided would also have the same sequence, thus correlating with the different categories. Other data include a unique identifier that correlates with the answers provided by the participant. The main objective of the questionnaire data is to determine the current knowledge levels of the participants: this is achieved by determining if the answer provided is correct.

### **7.3.3.2 Online Game**

The data generated in the online game was used for multiple purposes, which included tracking the progress of the participants and measuring the understanding of the information security awareness topics. The data generated during the game play was stored in a database. The online game also used the stored data to display the questions, each of which belonged to a category related to an identified security topic. The random events were generated by the online game and stored as part of historical data and enhanced the features of the game. The responses created by the participants were stored and compared against the stored correct answers. This was used as a mechanism to score points to determine the leader within the sample, and also to determine which categories (topics) the participants performed better in: in other words, the identification of which information security-related topics needed to be focused on to improve the total information security awareness within the identified group. The tracking data was used to determine how long the participant took to answer each questions and how many questions were answered. This was achieved programmatically by having a timer running from when the question is displayed to when the question is answered. Network latency did not affect the study due to the location of the participants: the study was conducted in the same location, and hence network latency-related issues would affect all the participants equally and would not skew the data about the time the participants took to answer the questions.

## **7.4 Limitations**

The research instrument used does limit the data collection to a controlled environment, namely a single location and limited to one day. The online game uses a network and network latency would affect the tracking feature of the game, which determines how long the participant takes to answer a question. In addition, having participants from multiple locations accessing the game during any period of the day introduces uncertainty in the results because participants could have received help to answer the questions from friends or other online resources.

The use of quantitative data limited the findings to the results from the questionnaires. Multiple-choice questions have an inherent flaw because it is possible for participants to guess the answer correctly. If four options are available then the participant has a 25% chance to randomly select the correct option. The use of qualitative data could have

supported the hypothesis that gaming could reinforce learning by repeating the content to the participant. Furthermore, interviews could also have been used to support the findings from the quantitative data. For example, if the quantitative data showed that information security knowledge had increased, interviews could have been used to support the findings.

The data was collected in one day. The amount of knowledge transferred during the limited time could have affected the knowledge retained. Although breaks were given to assist in concentration management, many participants could have lost interest and focus as the day progressed. Conducting the data collection over a period of at least two days would have been ideal. This would have allowed for assessing the retention of knowledge more accurately. The first day would consist of the initial pre-assessment and first post-assessment data collection, while the next day would be used to conduct a final data collection after the game play to compare against the findings after the last assessment on day one.

The use of one sample does limit the findings to a specific population. It would have been beneficial to collect data from another sample and compare the findings between the two groups. The size of the current sample also influenced the accuracy of the findings. Having a control group during the day of the collection who did not partake in the online game could have proven valuable, as this would have shown the significance of motivation. One sample was selected for the study due to the number of participants available for the study. Also, lack of time and funding limited the collection of data from the sample to one day.

A profile of the sample population is absent from the current study. The profiling would have provided a more accurate representation of the sample and could have been used to correlate with the pre-assessment data and other personality traits. For example, it could have determined what motivation indicators the group has. This would have been beneficial to understand what the effect of providing a reward for the game play would have had.

## **7.5 Ethical Consideration**

The ethical procedures followed during the collection of the data are described in this section. These are prescribed by the University of South Africa (UNISA) and described in the Ethical Clearance Document (University of South Africa 2007). It was a requirement to

obtain ethical approval from the School of Computing Ethics Committee before commencing with the research. UNISA promotes four established and accepted principles of ethics as bases for research. These are:

- Autonomy - The freedom, rights and dignity of the participants should be respected
- Beneficence - The work conducted in this study should contribute to society
- Non-maleficence - No harm should be done to participants
- Justice - Benefits and risks should be apportioned among society

These are addressed in the study as follows. The participants were informed at the start of the data collection that they could stop participating at any stage without giving any reason. This information is enclosed in the consent form provided to each participant before commencing with data collection (see Appendix F for the consent form).

Cybercrime has increased during the last few years and many uninformed computer users are unknowingly attacked in cyberspace. These attacks can be mitigated by equipping computer users with the required knowledge to protect themselves. This study contributes to society by transferring knowledge to become aware of cyberthreats and provide mitigation techniques for protection.

The participants were required to attend a training session and conduct work on a computer. None of these posed a threat to harm the participants. Breaks were provided during the data collection to ensure participants have an opportunity to recover mentally. All the participants were exposed to the same content; hence no individual or group got special treatment for example, providing additional training material to selected individuals.

It is an important aspect to ensure that the participants were fairly selected. The first 40 participants that signed up to participate in the study were selected. The Department for Computer Science and Information Systems at the University of Venda was contacted to inform the students (the participants) about the study. A briefing session was held with the lecturers to ensure that all the relevant information was explained and understood. A hard copy containing the background information of the study was provided to each lecturer. The lecturers were responsible for informing each of the selected students. A list was kept with the secretary of the department, which was easily accessible, for the students to indicate willingness to participate. The social, cultural and historical backgrounds of the participants were also considered. This was achieved by selecting a university in a rural

area that was not located close to a well-developed city. The students also would not have information security content addressed in any of their under-graduate modules.

The participants were compensated during the data collection process and were given beverages and food. A meal was packaged before the data collection day to ensure that all participants received equal portions. Furthermore, inducements in the form of prizes were provided during the online game playing. The terms and conditions of the inducements were explained to each participant. An incentive was provided to encourage the participants not to merely answer the questions as quickly as possible. The game play was essential to the outcome of the study and focus was required. A scoring system was built into the game to determine the winner; the user with most correct answers after the completion of the game is the winner. Another feature built into the game determined random winners during the game play apart from the main prize.

Each participant had to read and sign the consent form before starting with the data collection. This consent form declared the purpose of the research; the risks and benefits; the method used to collect the data; the identity of the researcher; why the participants were selected; measures taken to ensure privacy, anonymity and confidentiality; plans for future use of information; the right not to participate and to withdraw; the right to get help and request additional information, if required to assist in the decision to participate (Appendix F). Hard copies of the consent form were created and handed out to each participant. The consent form was then discussed with the group.

Each point was explained and the participants were provided with opportunities to ask for clarification of any point not understood. The participants who agreed with the consent form signed it. Each consent form was collected individually from each participant. This is required to ensure to create a safe environment for the participants, who may be shy and afraid to ask question within groups. The participants were all asked to leave the venue. This allowed the participants who did not want to continue with the study to leave without the fear that the rest of the group would identify them.

It is important to note that permission had to be obtained to use students from the tertiary institution where the participants are currently completing their studies. All the stakeholders were contacted to establish the required process to use students from the institution in this research. The Deputy Vice Chancellor from the University of Venda was informed about the acceptance of the ethical clearance received from UNISA, and



permission was granted to continue with the study. The selection of the students commenced once the approval to continue was received as well as the selection of the data for the information security awareness program.

The participants' privacy, anonymity and confidentiality were maintained during the study. The data collected was stored in a database. Authentication processes were used to ensure restricted access to the data. Each participant was provided with a unique number which was used during the data collection. This was implemented to protect the identity of the participant. The game was accessed using the authentication system of the social networking site. A record of the participant was captured in the game's system to keep a record of the questions completed and assist in the identification of the winner of the prizes described earlier. This information does not correlate to the survey information; hence no participant identities can be inferred. All data collected during the study was destroyed from each storage platform, which includes digital and physical devices. The data was stored at a central location and a backup was made to another location. Storage at each of these locations is encrypted. The data is securely stored at two locations. This minimises the risk of leaking data due to negligence as these devices are small and could easily be stolen or lost.

It should be noted that all reasonable attempts have been made to protect the participants and adhere to the ethical guidelines prescribed by UNISA.

## **7.6 Conclusion**

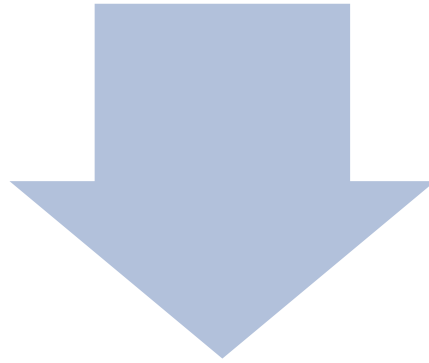
This chapter discussed the implementation of the third phase of the NIST information security awareness framework. The development of an autonomous system to conduct information security awareness training was proposed in Section 6.2. A target group was identified to participate in the information security awareness program, to test the hypothesis that gaming would be an effective component within a security information awareness programs. Various methods to collect data were analysed and the most effective method was selected. This resulted in the design and development of the research tool to be used within this study. A schedule was subsequently created on how the information security awareness program would be implemented and potential risks were identified. Due to the collection from a human sample group, ethical considerations were addressed.

In addition, the prototype game described and designed in Section 6.3 was customised for the data collection during the information security awareness program used for this study. Improvements to the initial design considerations were identified and used in the development of the online game. This iterative process ensures that knowledge acquired during prototyping can be used to improve future implementations.

The next chapter discusses the findings from the data collected during the information security awareness program. The findings can be used as part of the post implementation phase of the NIST information security awareness program to subsequently improve the information security awareness program.

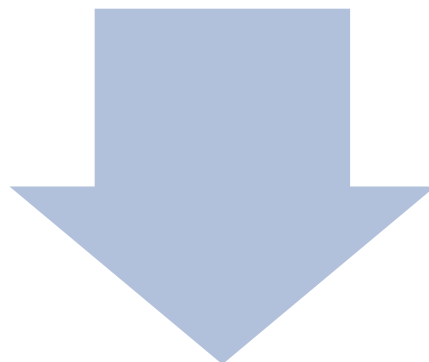
## Chapter 8: Post Implementation (Analysis of Data)

Chapter 7 - Implementation (Data Collection)



## Chapter 8 - Post Implementation (Analysis of Data)

- 8.1 Introduction
- 8.2 Analysis
- 8.3 Findings
- 8.4 Conclusion



Chapter 9 - Conclusion

Figure 8-1: Layout of Chapter 8

## **8.1 Introduction**

The previous chapter addressed the implementation phase of the information security awareness framework proposed by NIST.

A need was identified for an information security awareness program at a university. Topics relevant to the environment were identified from research conducted on threats originating from shared resource environments and social media. An online game component was designed, developed and deployed as part of an information security awareness program. Data was collected from the participants to measure the effectiveness of a social networking game, hopefully resulting in an increase of the participants' information security awareness.

This chapter discusses the analysis of the collected data as part of the final phase of the NIST information security awareness framework. The data sets include results from the questionnaires which formed part of the assessments, as well as the data generated by the game.

The findings are presented in Section 8.3. These findings are used as a mechanism to update the design and improve the information security awareness program.

## **8.2 Analysis**

This section describes the analysis of data collected through the questionnaires and the online game. The main objective of this section is to summarise the collected data to provide meaning.

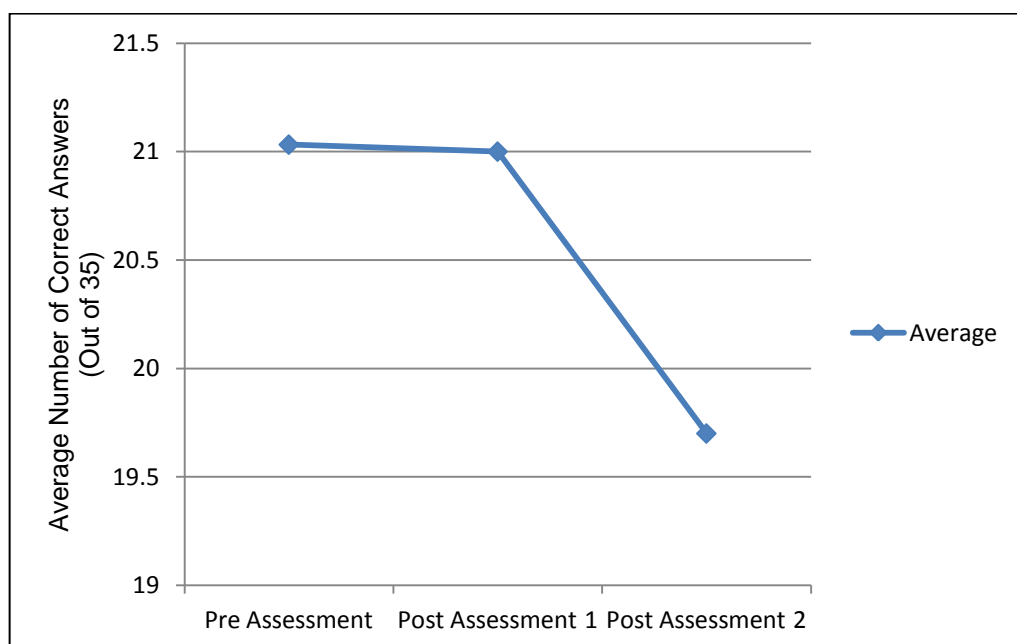
### **8.2.1 Analysis of the questionnaire data**

The statistical methods used to analyse the questionnaire data are described in this section. The aim of the analysis is to determine whether the group's information security awareness increased during the playing of the game. This was achieved by calculating the average group marks after each questionnaire.

The number of correct answers was determined for each survey (the pre-assessment, the first post-assessment and the second post-assessment). The average number of correct answers for each questionnaire was calculated: the results are depicted in Figure 8-2. The first questionnaire (pre-assessment) was used to create a baseline of the initial information security awareness levels to measure the other questionnaires' results against. This resulted in demonstrating the impact of the training session and the online game. The

second questionnaire (post-assessment 1) was done after the training session while the last questionnaire (post-assessment 2) was administered after completing the online game. Each questionnaire consisted of five questions from the seven categories resulting in 35 questions per questionnaire.

The pre-assessment indicated that the participants scored an average of 21.03 correct answers out of the possible 35 correct answers. In the second questionnaire (post-assessment 1), the participants' scores averaged 21. The last questionnaire administered after the online game resulted in an average score of 19.7 out of a possible 35 marks.

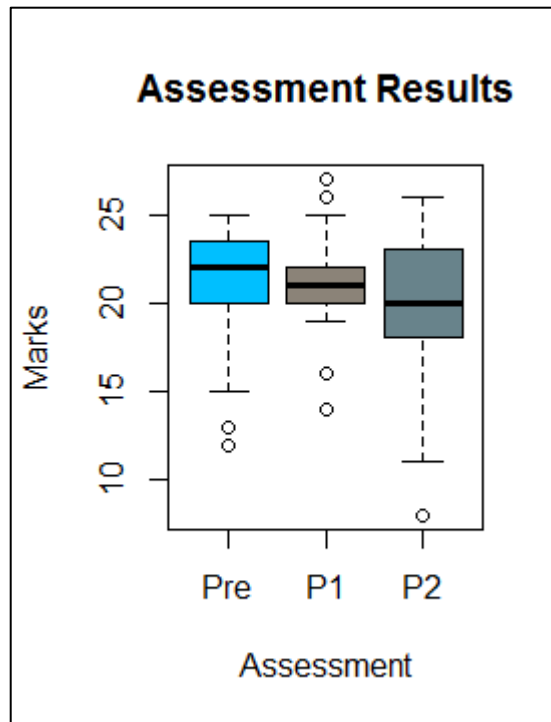


**Figure 8-2: Questionnaire Results (Average) (Source: Own)**

The results from the questionnaires show a decrease in the information security awareness of the participants. The information security awareness knowledge remains relatively consistent between the baseline (21.03) and after the completion of the training session (21). The decrease of 0.3 is negligible. Surprisingly the result of the final questionnaire was 19.7. An increase in the average points was expected, not a further decrease of 1.3 points after the completion of the online game. The reason for this will be explored in the next section.

Outliers could have affected the results and need to be removed from the current results to observe if the results are not skewed by them. The outliers can be trimmed from the data before calculating the mean. As the questionnaires counted out of 35, the maximum a participant could obtain is 35 marks. The graphical distribution of the marks obtained by all

participants for each assessment is depicted in Figure 8-3 and Figure 8-4. A box plot graph (Figure 8-3) and a plot graph (Figure 8-4) were generated from the analysed data. The data represents the marks received by all the participants of the pre-assessment (Pre), post-assessment 1 (P1) and post-assessment 2 (P2).



**Figure 8-3: Assessment Box Plots (Source: Own)**

Box plots are used to display differences between the assessments. Box plots have various advantages which include displaying the full range of the variances (from maximum to minimum values), the median (indicated by the thick black line), and outliers (McGill, Tukey & Larsen 1978). The different assessments' box plots are depicted in Figure 8-3 and the following observations are made:

- Pre-Assessment (Pre) – Most of the marks obtained are between 20 and 24 out of 35. These marks form a baseline which is used to compare the results against the other assessments.
- Post Assessment 1 (P1) – The assessment after the training session shows a small variance between the minimum and maximum value. Also, a small decrease in the median is noticed compared to the median of the pre-assessment (Pre).
- Post Assessment 2 (P2) – A significant variance between the minimum and maximum values is noticed, as well as a further decrease in the median.

Next the data was also graphically displayed with the use of a plot graph. The use of the plot graph not only makes the outliers clearly visible but also depicts the distribution of marks received by each participant (Figure 8-4). The horizontal axis indicates each mark obtained by each participant for the different assessments. The item values of S001 through to S031 depicted on the horizontal axis denotes each individual participant. In other words, each respondent's marks for each assessment are depicted in Figure 8-4. Also the distributions of the marks are visible and the grouping for each assessment would present the author an opportunity to conduct preliminary analysis on the dataset.

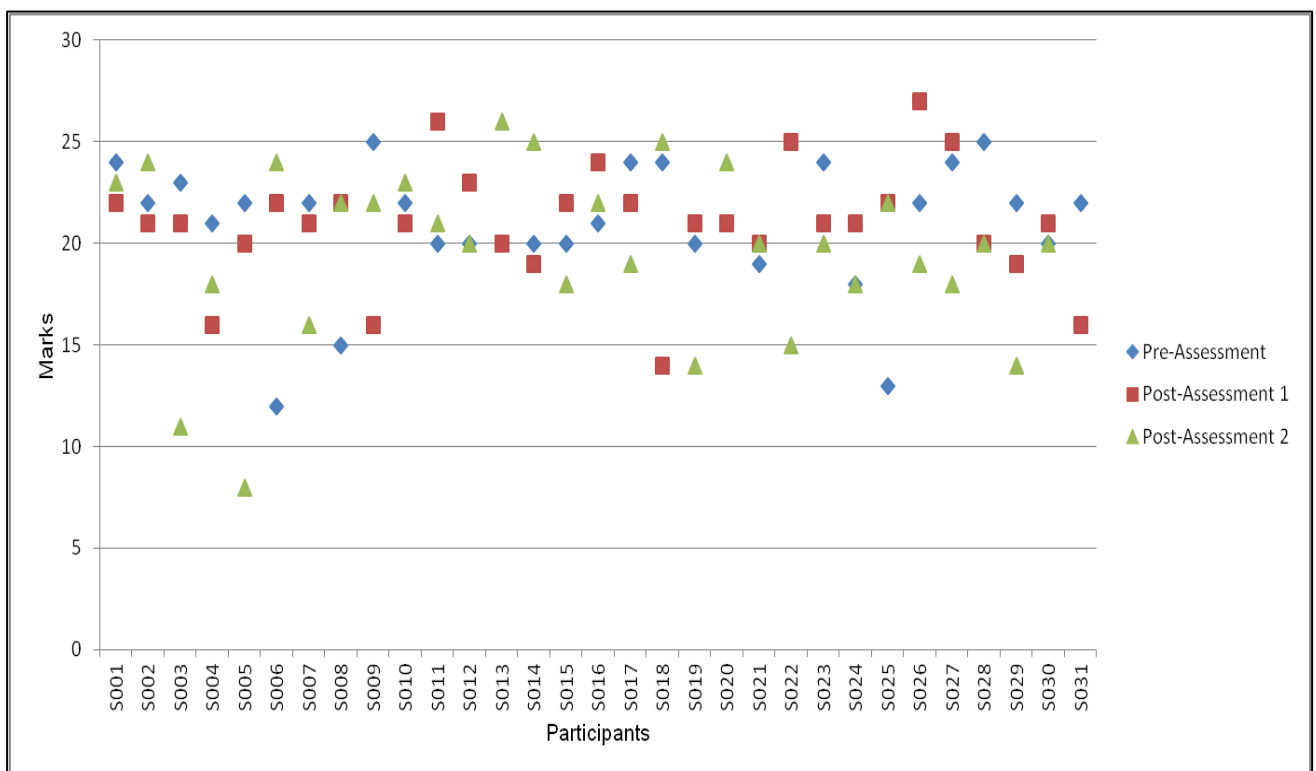


Figure 8-4: Distribution of Assessment Marks (Source: Own)

Subsequently the identification of outliers is possible. The distribution of marks per assessment provides the ability to comment on the effect of the assessments on the participants. The first observation notices that marks for the pre-assessment (Pre) and the first post-assessment (P1) were less staggered than the second post-assessment (P2). In other words, the marks for the pre-assessment (Pre) and the first post-assessment (P1) are more closely grouped together than the marks for the second post-assessment (P2).

Another observation is that the marks for pre-assessment (Pre) and the first post-assessment (P1) are mostly grouped in the 20 to 25 mark region, while the marks for the second post-assessment (P2) tend to appear in the 15 to 20 mark region. This shows that

the participants' marks decreased during the second post-assessment (P2), indicating the participants were negatively affected between the first post-assessment (P1) and the second post-assessment (P2).

Microsoft Excel was used for the analysis of the data. The MEDIAN and TRIMMEAN functions were used. The MEDIAN function is used to calculate the value that is in the middle of a set of numbers; in other words, half the numbers have values above the median, and half have lower values (Microsoft 2014a). The TRIMMEAN function calculates the mean taken by excluding a percentage of data points from the top and bottom tails of a data set (Microsoft 2014c). The most extreme 20 percent of scores were removed, the highest 10 percent of scores and the lowest 10 percent of scores, before calculating the mean. Figure 8-5 depicts the comparison between the mean and the trimmed mean for each of the surveys. The graph shows a more substantial decrease in the average points between the pre-assessment and the first post-assessment when the outliers are removed. Therefore the outliers have an impact of the calculation of the mark for the pre-assessment. The trimmed mean calculations between the pre-assessment and the first post-assessment highlights the training session had little effect on the learning of the participants. However, both results between the first post-assessment and second post-assessment for the mean and trimmed mean have the same shape, which also indicates a decrease in marks after completion of the online game. An increase in marks between the first post-assessment and second post-assessment were expected subsequently supporting the hypothesis that the game has a positive learning effect. Conversely the impact of the gaming session is found to have had a negative impact on learning. Further analysis of the gaming component is required to determine the causality of the decrease in marks.



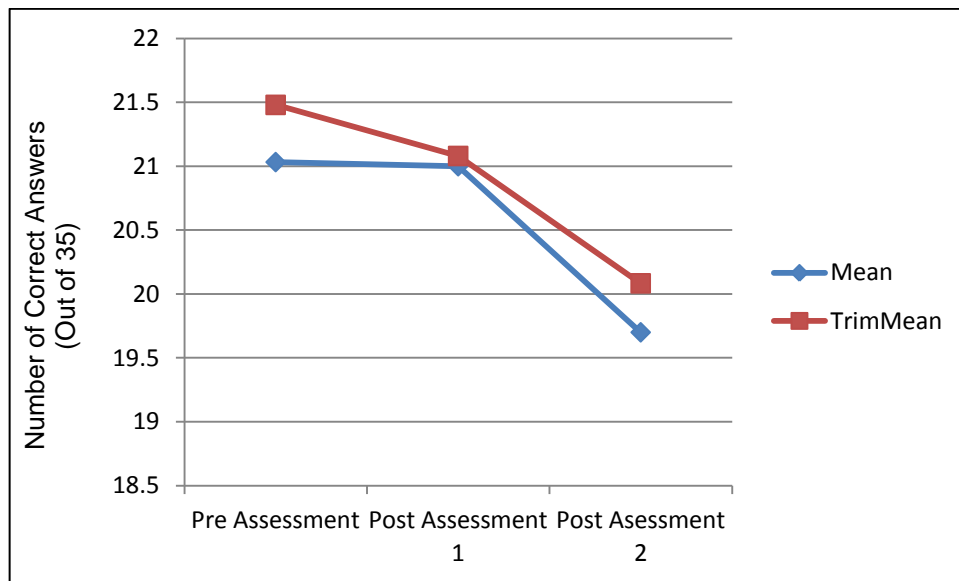


Figure 8-5: Line Graph Comparing Results (Mean and TrimMean) (Source: Own)

The mean is useful to summarise a group of numbers but is sensitive to extreme values created by outliers. Next we calculate the median as it calculates the value that is in the middle of an ordered set of numbers and is seen as a more robust value within a dataset which is not affected by outliers. The calculated median values for all the surveys are depicted in Figure 8-6. The values for the pre-assessment, the first post-assessment and the last assessment are respectively 22, 21 and 20. These results also indicate a decline after the completion of each questionnaire.

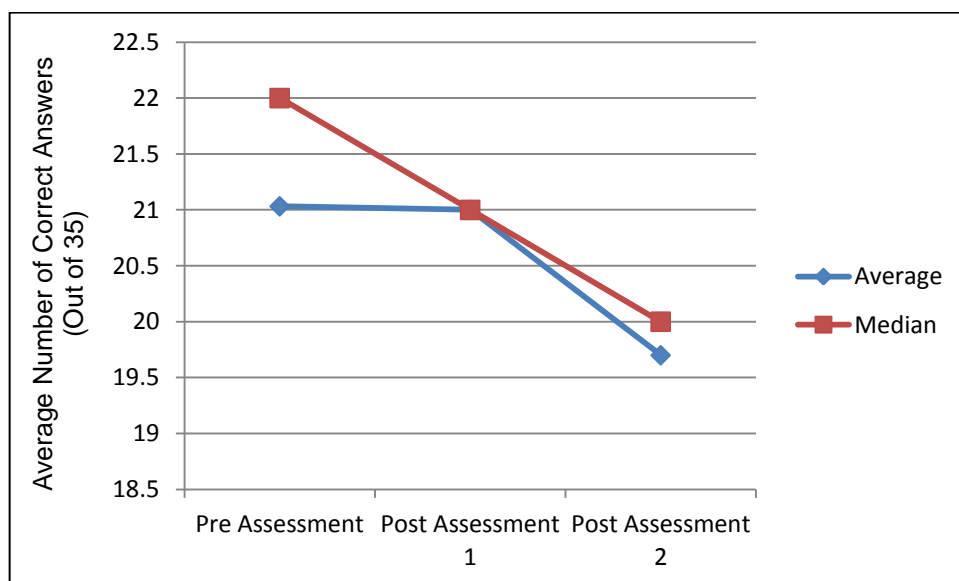


Figure 8-6: Line Graph Comparing Results (Mean and Median) (Source: Own)

The variations in each questionnaire's results are calculated next. Although the previous analyses have shown a decrease in information security awareness levels, after each

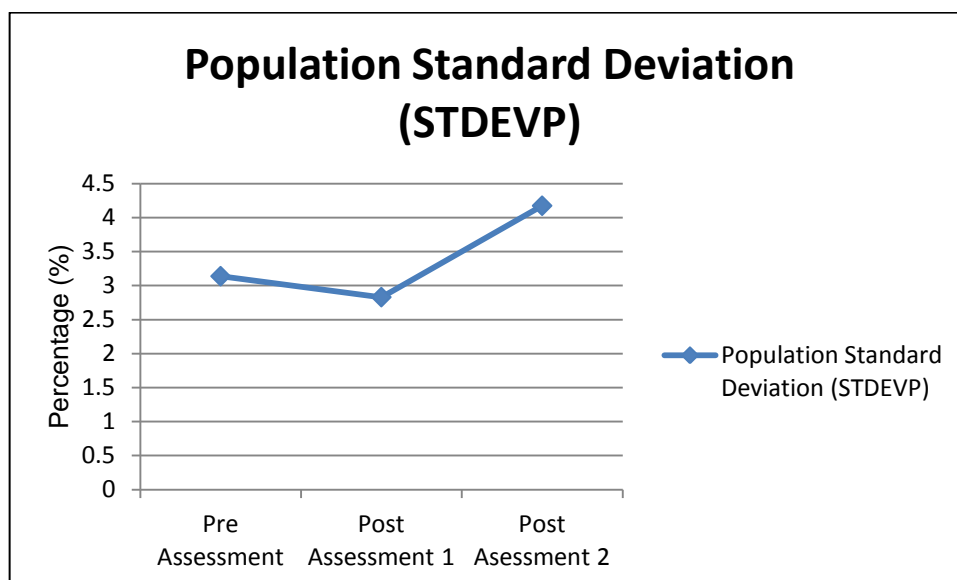
questionnaire the results of the variation analysis could indicate the impact of the training session and participating in the online game. The bigger the difference between the mean values, the higher impact an activity had on the participants. The standard deviation of the population is depicted in Figure 8-8. This was calculated using the STDEVP function in Excel (the formula is depicted in

Figure 8-7). The STDEVP function measures how far values are spread from the mean (average value) (Microsoft 2014b). The “ $n$ ” denotes the number of participants, the “ $x_i$ ” represents the individual values while “ $\bar{x}$ ” represents the mean.

$$\sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n}}$$

**Figure 8-7: Formula for STDEVP (Microsoft 2014b)**

Therefore the line graph shows that the biggest deviation between the questionnaire results occurs between the second and third questionnaires, which are respectively the first and second post assessment. The activity that occurred between these two questionnaires is the online game which the participants played.



**Figure 8-8: Line Graph Population Standard Deviation (Source: Own)**

The variation on the population (VARP) function in Excel was used to calculate the variance based on the entire population (Microsoft 2014d). The formula for the VARP function is given in Figure 8-9. This was used to validate and support the results from the population standard deviation. The results from determining the variation on the population

for the three questionnaires is depicted in Figure 8-10. The variance between the baseline from the first questionnaire and second questionnaire are small, but the variance between the second and third questionnaire is substantial.

$$\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n}$$

Figure 8-9: Formula for VARP (Microsoft 2014d)

The line graphs for the variation and the standard deviation of the population have a similar trend which correlates with each other. The decrease in the average scores (deduced from the Mean, TrimMean and Median calculations), together with the results from the deviation calculations, indicate a significant deviation in the participant's information security awareness levels after the completion of the online game.

The data collected through the online game is analysed next, as from the results of the survey data it is clear that the game had an impact on the study.

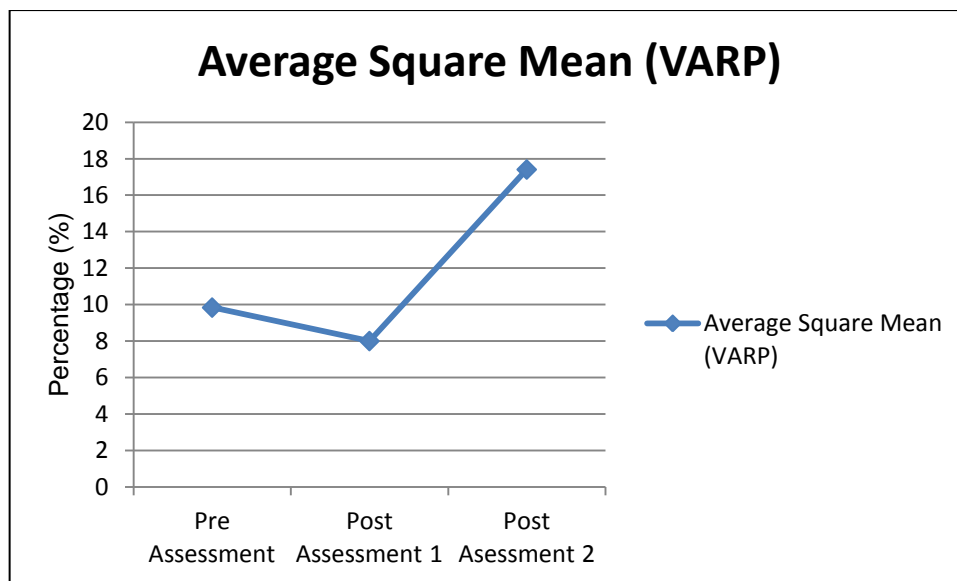


Figure 8-10: Line Graph Population Standard Deviation (Source: Own)

### 8.2.2 Analysis of the online gaming data

The online gaming item, as part of the questionnaire schedule, was also used to collect data during contact time with the participants. The online game had two functions: reinforcement of knowledge learned during the training session and the collection of data. The data collected was analysed to determine the following:

- How many responses were collected during the game play period?

- How many of these responses were correct?
- The response times of the participants

Figure 8-11 depicts the total number of responses from the participants who played the online game as part of the information security awareness training. The online game was deployed on a social networking site and is described in Section 7.3.1.5. The online game was played from 2:35pm and ended at 4:05pm. This constitutes a ninety-minute session for game play; the original allocated time frame was two hours (Table 7-3), but due to time constraints the duration of the session was reduced. Responses were captured to determine the number of correct responses as this was part of the gamification requirements for the game play. The response times were also collected as it was deemed beneficial to determine if there was a correlation between response time and the correctness of a response. A total of 2469 responses were collected within the time frame. These responses were grouped in 5 minute intervals. The following observations were made at the following time intervals:

- 2:35pm to 2:45pm: The initial 10 minutes show a slow response rate as many users were getting accustomed to the controls to play the online game. This period can be attributed to a learning phase in playing the game.
- 2:45pm to 3:15pm: A steady increase in responses is noticed during the next 30 minutes. As users got more accustomed to the game, they could focus on responding to the questions.
- 3:15pm to 3:20pm: A decrease in the number of responses is noticed; this was due to refreshments that were handed out to the participants during the game play session. The participants might have been distracted by the refreshments, thus losing the momentum achieved in the previous time intervals.
- 3:20pm to 3:40pm: An increase in responses is seen after the refreshments. This trend continues and has a steep increase in the last 5 minutes of the gaming session. The participants were trying to answer as many questions as possible to maximise the collection of points to be leader at the conclusion of the gaming session.
- 3:40pm to 4:05pm: A sharp decrease is attributed to the end of the gaming session, although some participants were still playing the online game. The majority of the participants stopped playing the online game at 3:40pm.

Figure 8-12 and Figure 8-13 provide a graphical illustration of the correct and incorrect responses collected during the online game play. Figure 8-12 shows a combined view of incorrect and correct responses. It is noticeable that during the game play more correct answers were provided. Figure 8-13 depicts correct and incorrect responses separately; it also clearly shows that the number of correct responses tends to be higher than the number of incorrect responses.

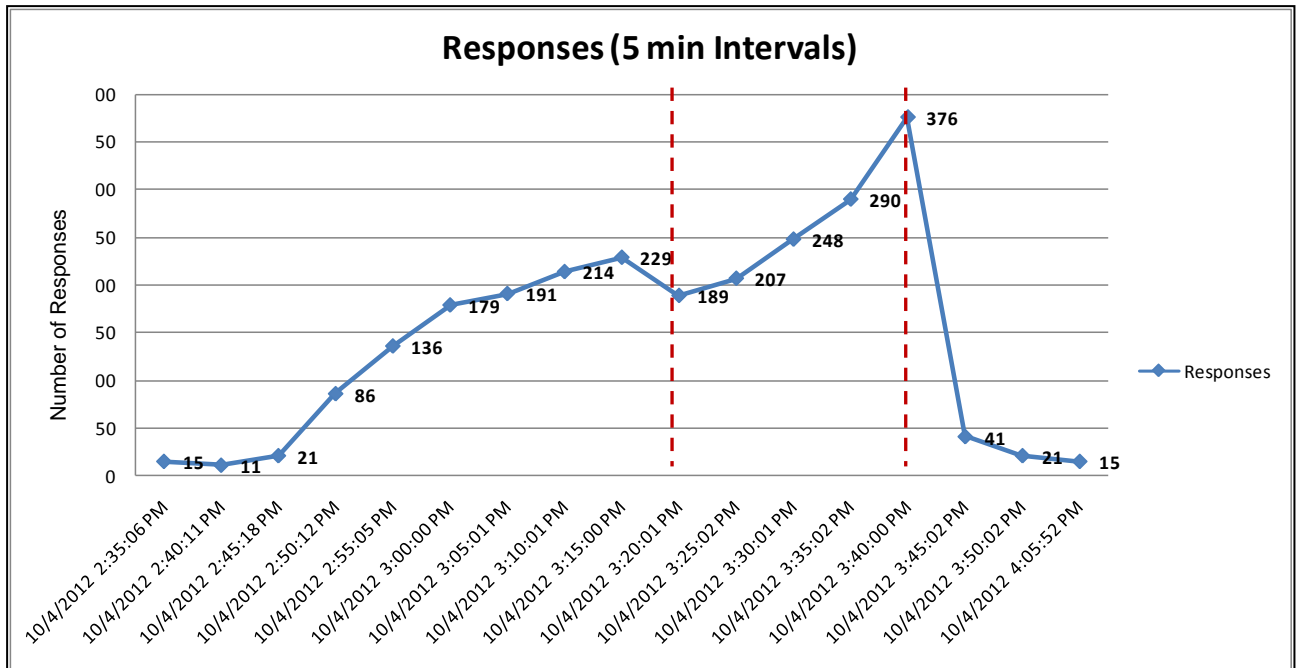


Figure 8-11: Total Responses (5 Minute Intervals) (Source: Own)

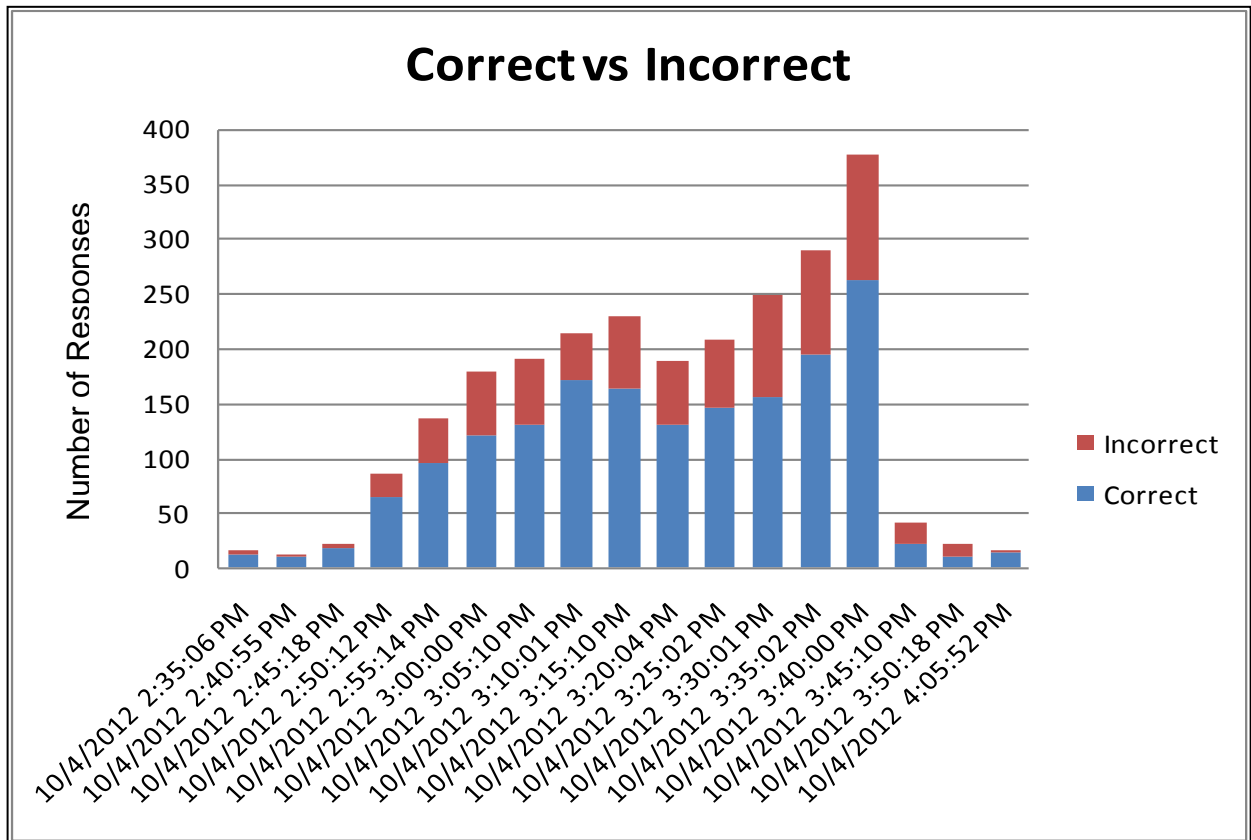


Figure 8-12: Response Classification (Correct and Incorrect Responses) (Source: Own)

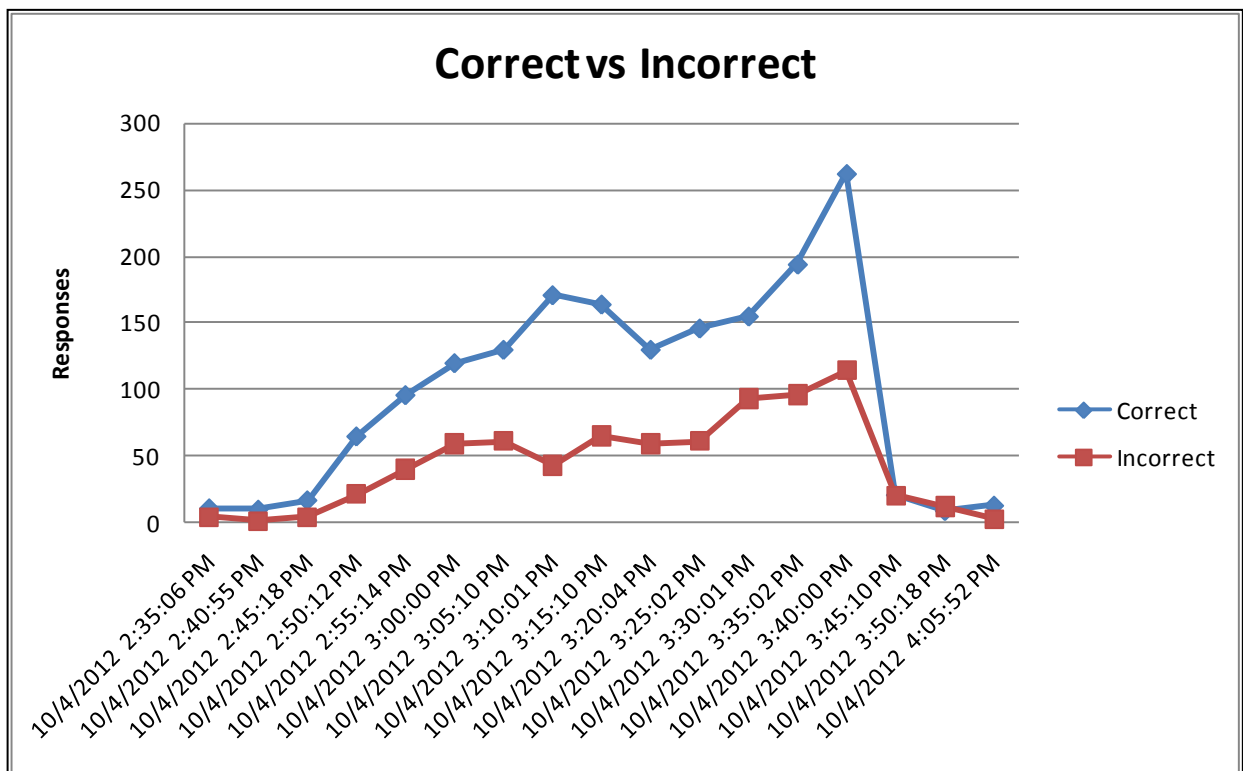


Figure 8-13: Correct and Incorrect Responses (Source: Own)

Furthermore, the correct responses increase over time intervals, while the incorrect responses are more consistent over time. This indicates that learning could have taken place during the game play. Another interesting observation can be made during the time interval from 3:20pm to 3:40pm, where a steep increase in correct responses was noted. The increase in responses should have increased the number of incorrect responses as well if the participants did not acquire awareness knowledge during the game play. The increase in correct answers (as opposed to incorrect answers) indicates that learning occurred during the gaming session.

The effect of “thin slicing” could also have played a role in the results. “Thin slicing” is using minimal information to make quick decisions (Ambady & Rosenthal 1992). The participants could have reinforced their knowledge about the information security awareness topics during the training session and while playing the online game. This was possible through feedback provided to the participants. In other words, the participants also learned while playing the online game. This was observed with the decrease in the response time once a participant answered correctly. This can be attributed to the participants not requiring processing of the information. In other words, the more a person knows about a topic, the less they need to think when answering questions about the topic. This is also evident during the online game which the participants played. They were also extrinsically motivated by the reward provided for winning the online game. As a result, the data not only showed quicker responses but also an increase in correct answers while the response rate increased. Consequently, as the participants wanted to earn more points their number of responses increased and they took less time to answer the questions.

The graph depicted in Figure 8-14 shows the average time the participants took to answer questions. The five minute time intervals were used to show the average time participants took when making correct and incorrect responses.

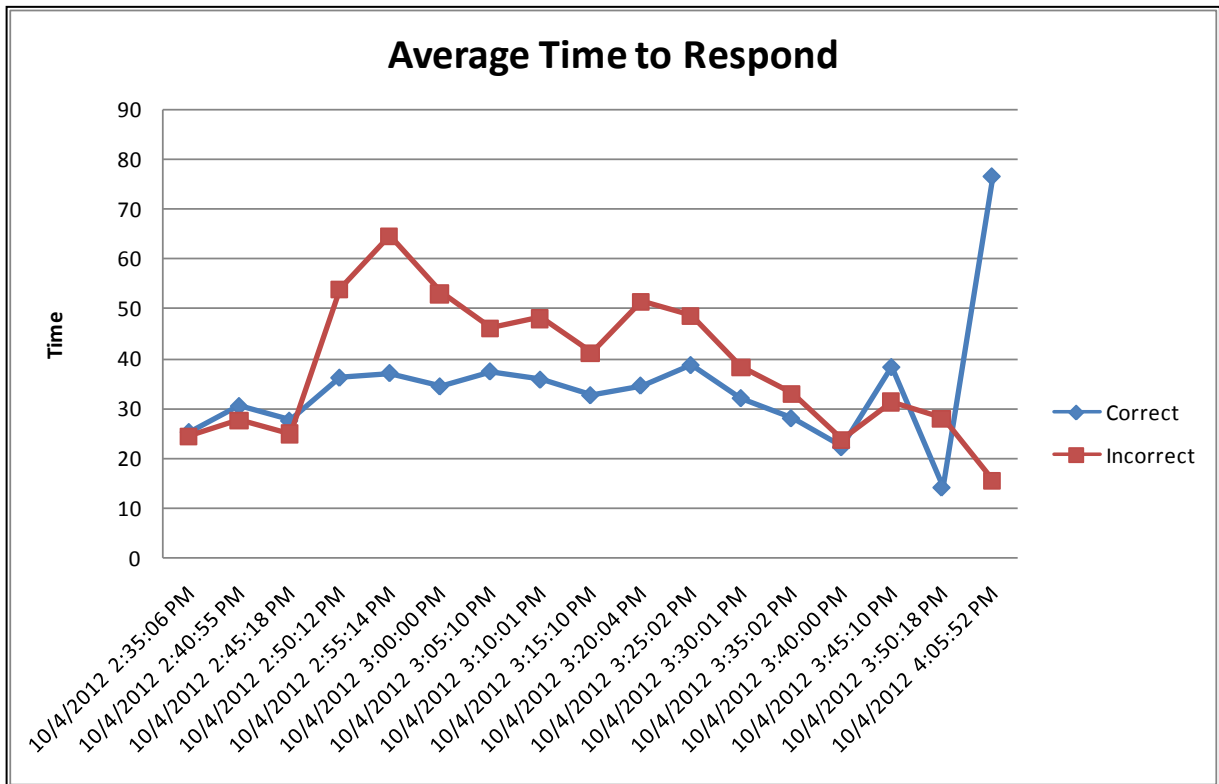


Figure 8-14: Average Response Time (Source: Own)

The following interesting observations were noticed from the data collected:

The average response time for correct responses were lower than the response time for incorrect responses at most of the time intervals, hence participants who answered correctly take a shorter time to answer than participants who answer incorrectly.

The graph shows a consistent response time for correct answers, while the response times for incorrect responses are more erratic. The incorrect responses could be interpreted as participants not knowing the answer and trying to analyse the question and the possible options before responding. The consistent response time for correct answers could be ascribed to participants having the knowledge to answer the question correctly.

The time frame between 3:20pm and 3:40pm shows an increase in responses (Figure 8-11). This could be attributed to the participants answering questions in the online game to collect points in order to become the leader and win the prize. This also resulted in participants taking a shorter time to respond to questions. Interestingly, the average times for correct responses were still shorter than for the incorrect answers.

Deeper analysis of the data collected from the online game is tabulated in Table 8-1. It shows categorically which topics were presented to the participants to answer. It should be



noted that the online game randomly selected questions from the available question test bank. The online game programmatically ensured that questions were not repeated to the same participant during the game.

**Table 8-1: Online Gaming Topic Response Distribution**

<b>Description</b>	<b>Number of Correct Responses</b>	<b>Correct Responses (%)</b>	<b>Number of Incorrect Responses</b>	<b>Incorrect Responses (%)</b>	<b>Total Number of Responses</b>	<b>Number of Responses (%)</b>
Phishing	208	12	116	15	324	13
Browser	170	10	59	8	229	9
Social Networking Sites	391	23	142	19	533	22
Cyberbully	168	10	89	12	257	10
Malware	272	16	49	7	321	13
Passwords	430	25	182	24	612	25
Spam	73	4	116	15	189	8
	<b>1712</b>		<b>753</b>		<b>2465</b>	

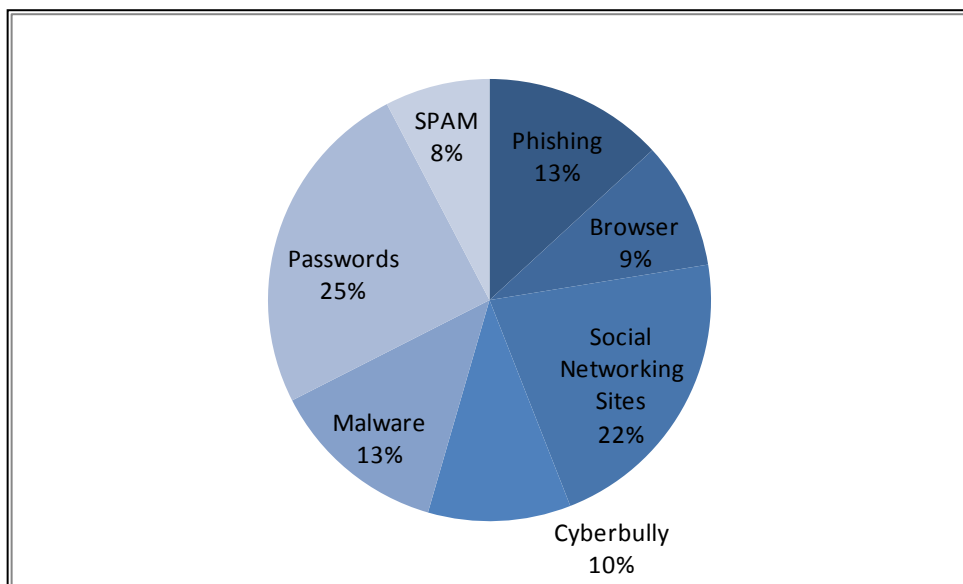
Questions from the password topic were presented to the participants the most (25%) and spam the least (8%). The questions answered correctly (25%) and incorrectly (24%) the most also were from the password topic. This could be attributed to the number of questions available for the password topic. However the least number of correct responses (4%) were for the spam topic but this could be due to the low number of questions available. A significant observation is the least number of incorrect answers (7%) were from the malware topic as a high number of questions on malware were presented to the participants. Therefore the participants demonstrated a better understanding on the topic of malware.

A total number of 2465 questions were displayed to the participants: of these, 1712 were answered correctly and 753 were answered incorrectly. Almost 70% of the questions presented to the participants were answered correctly.

This is significantly higher than the approximated averages of 60% for the questionnaire results of the first and second questionnaire. The questions used in the questionnaires and the online game covered similar security-related topics. The 10% improvement in the group of participants can be attributed to them learning about the topics through reinforcement and using gaming as a platform. The knowledge of the topics contributed to

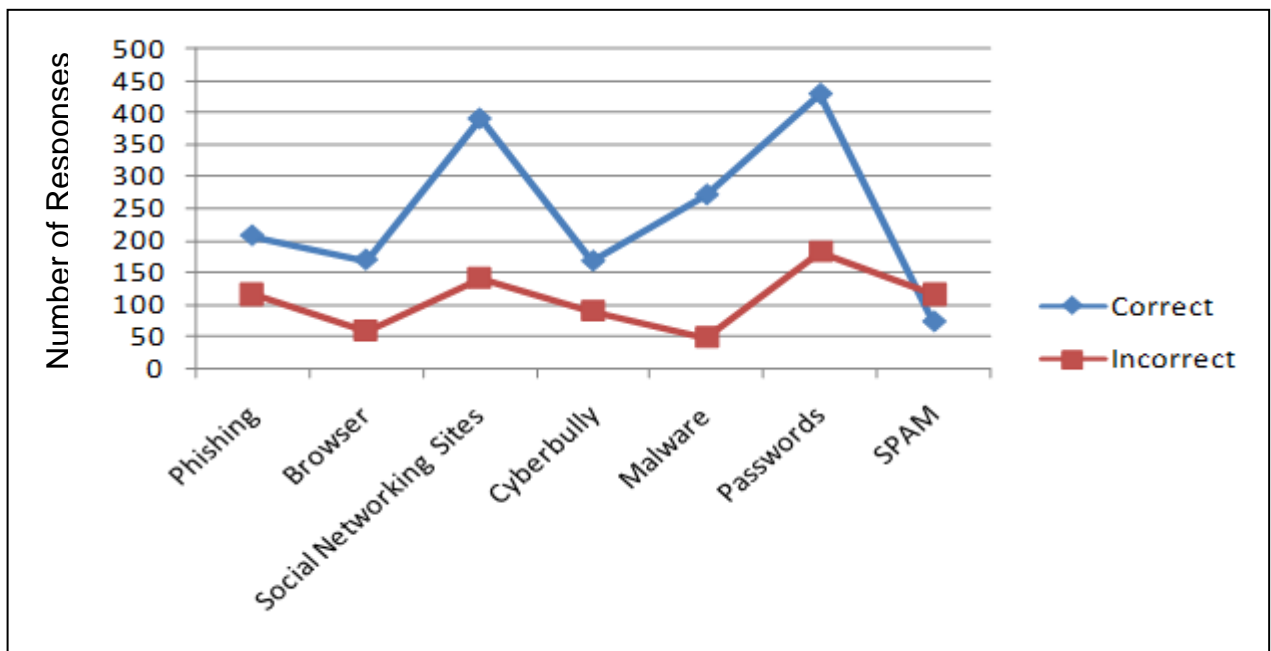
the participant's success in the game, which was aligned with the immediate goal to win the game and receive a reward. On the other hand, knowledge acquired during the training session did not contribute to an immediate goal. In other words, the participants did not see the gain of paying attention during the training session, while during the online game the focus was on winning the reward by answering the questions correctly.

Figure 8-15 depicts the distribution of the topics that were presented to the participants during the online game. The breakdown shows that the Password (25%) and Social Networking Site (22%) questions were required to be answered most often, while Spam (8%) and Browser (9%) questions were presented least often during game play. The questions presented to the users were randomly selected from the database. This ensured that the same question was not displayed to users who sat next to each other.



**Figure 8-15: Distribution of Awareness Topics (Source: Own)**

The correct and incorrect responses collected after the completion of the online game are illustrated in Figure 8-16. More correct answers were submitted for all the information security awareness topics, except for the topic on spam. This shows that the participants did not understand this particular topic. Furthermore, the spam topic questions were the questions that were presented least often to the participants (Figure 8-15). After the completion of the information security awareness program, findings like these should be addressed by a follow-up training session that focuses on spam.

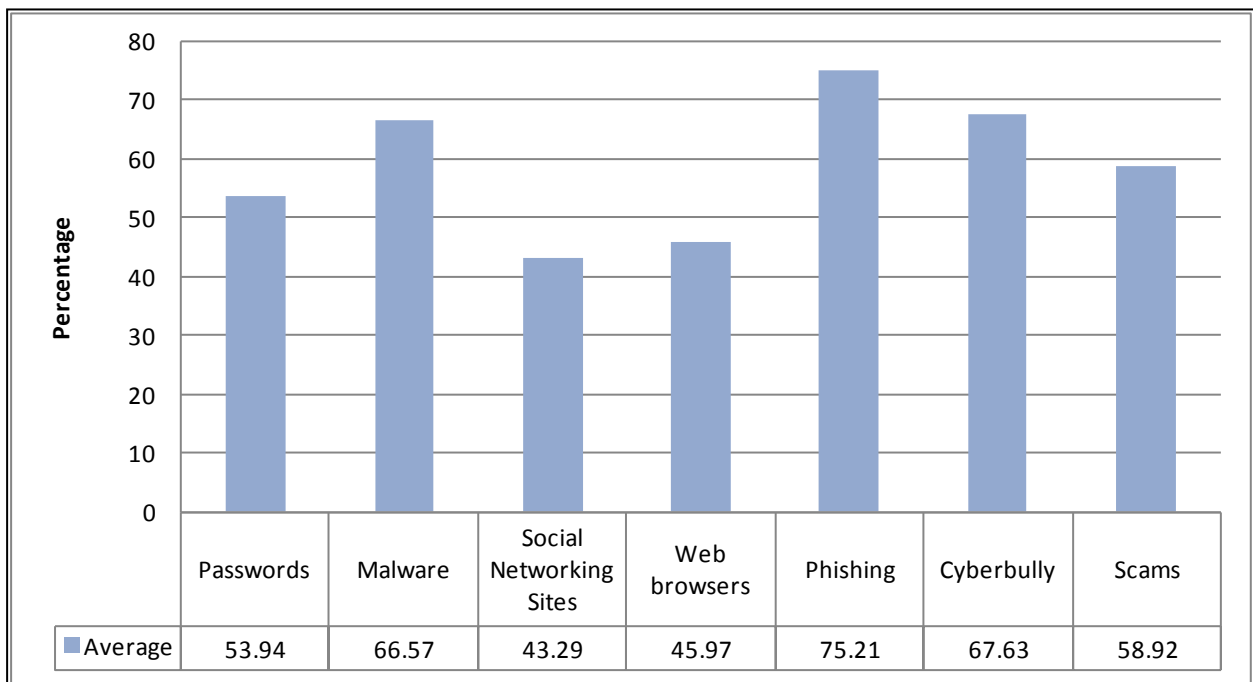


**Figure 8-16: Line Graph of Correct and Incorrect Responses for each Topic (Source: Own)**

It should be noted that the spam topic is part of the online game question database and the questionnaire topic was not named 'spam' but 'scams'. During the training session, the module on Phishing covered Phishing, Scams and Spam. Therefore the possibility exists that the participants confused the two different topics. An interesting observation was the average obtained for spam (39%) during the online game correlates with the average calculated for the last questionnaire spam topic (40%) (Table 8-2). This can also be seen with the Cyberbully topic but not with any other topic. The Cyberbully topic scored an average of 70% for the last questionnaire and scored a 65% during the online game.

**Table 8-2: Topic Breakdown for each Questionnaire**

Category Name	Pre Assessment		Post Assessment 1		Post Assessment 2		Overall Average (%)
	Average	%	Average	%	Average	%	
Passwords	2.65	52.9	2.61	52.26	2.83	56.67	53.94
Malware	4.06	81.29	3.35	67.1	2.57	51.33	66.57
Social Networking Sites	1.9	38.06	2.29	45.81	2.3	46	43.29
Web browsers	1.71	34.19	2.419	48.39	2.77	55.33	45.97
Phishing	3.39	67.74	4.16	83.23	3.73	74.67	75.21
Cyberbully	3.94	78.71	2.71	54.19	3.5	70	67.63
Scams	3.39	67.74	3.45	69.03	2	40	58.92



**Figure 8-17: Average Scores for Topics (Questionnaires) (Source: Own)**

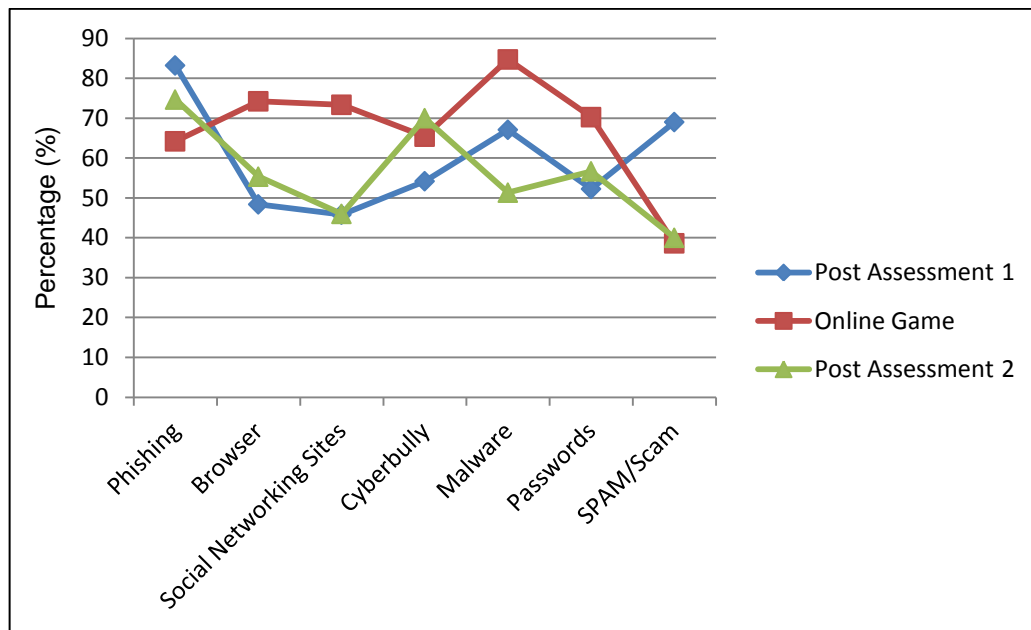
The results from the second questionnaire, online game and the last questionnaire were compared to determine if the online game had an influence on the results for the last questionnaire. This would be the case if the results of the last questionnaire (post-assessment 2) showed that each of the topics scored higher than the second questionnaire (post-assessment 1) topics. The result of this comparison is depicted in Figure 8-18.



**Figure 8-18: Comparison of average scores per Questionnaire for each Topic (Source: Own)**

This clearly shows the participants performed extremely well during the online game, as most of the topics scored significantly higher than the questionnaire results. One could argue that the participant’s information security awareness levels rose while playing the online game.

It is noticeable that there is no correlation between the topics of the questionnaire results used during the assessments (the green and blue lines in Figure 8-19). In other words, some of the topics improved while other worsened. This is supported by comparing the averages between the different questionnaire results, which clearly shows a decrease in the average score, as discussed earlier in this chapter.



**Figure 8-19: Comparing Post Assessment 1, Online Game and Post Assessment 2 Results (Source: Own)**

Therefore it seems as if the online game did not have an influence in increasing the information security awareness levels. The participants obtained results higher than the questionnaire results except for the last questionnaire.

These results were not expected. Specifically, the information security awareness levels should have increased after the training session and increased even further after the game play. The next step would be to determine the factors which contributed to these unexpected results.

The high level data collection process starts with a questionnaire, called the pre-assessment, to determine the baseline (the current information security awareness levels of the participants). Next, a training session is presented to the participants on the identified security topics. This is followed by a questionnaire, called the post assessment 1, to determine if the training session had an effect on the information security awareness levels. In this case, the results between the first two questionnaires were almost identical.

Following this, the participants played an online game which reinforced the concepts of the security topics. Analysis of the online game showed an increase in security awareness levels. The last step of the data collection was to use the final questionnaire, called the post-assessment 2, to again determine the information security awareness levels, but the results showed a substantial decrease and not the expected increase.

The event that influenced the outcome is located between the online game and the last questionnaire. Delving deeper into the data collection process it was found that a monetary reward was handed over to the winner after the completion of the online game. The reward was originally scheduled to be handed over after the completion of the last questionnaire. The reward was however handed over to the winner after the game play component.

Work conducted by Deci (1971) found that intrinsic motivation decreases when monetary rewards are used as an external reward for an activity. Ryan and Deci (2000) describe motivation as follows:

*“To be motivated means to be moved to do something. A person who feels no impetus or inspiration to act is thus categorised as unmotivated, whereas someone who is energised or activated toward an end is considered motivated.”*

Deci’s study consisted of 24 participants who were divided into two groups. 12 participants were placed in a control group and the others in the experimental group. The participants were asked to complete puzzles, in configurations provided by the researchers, in an hour-long session over three days. The time to complete each configuration was measured and recorded.

The experimental and control group completed the same puzzles on the first day. The experimental group was paid money for each configuration on the second day while the control group completed the configurations without any payment. On the final day, all the groups were asked to complete as many configurations without any remuneration.

Their findings showed that the control group was consistent in the time they completed the puzzles. However, the experimental group increased the number of puzzles completed when they were provided with monetary rewards while the number of puzzles completed substantially decreased when the rewards were removed. The results of these studies resemble the findings discussed in Section 8.2.1, although the use of a control group was not considered for this study due to constraints.

This phenomenon was also found by Kruglanski, Friedman and Zeevi (1971) who conducted research on a group of 32 participants to measure the effects of extrinsic incentives on qualitative aspects of task performance, including knowledge recall, creativity and task enjoyment. They found a higher quality of task performance and motivation when no extrinsic incentive is available. This implies that an external reward affects the performance of the participants.

The impact of motivation is a significant finding. This study did not take the effect of intrinsic and extrinsic motivation into consideration during the design phase. Future implementation would include qualitative data to measure the impact of motivation.

### **8.3 Findings**

This section describes the findings from the data collected during the information security awareness program described in this dissertation. The main focus of this research was to determine if the playing of games has an effect on knowledge transfer within the subject field of information security awareness. The field of computers, especially information security, is perceived as difficult and technical. With the high adoption of computers within society, the need to address information security awareness has also increased. Many examples exist that indicate cybercriminals are targeting unsuspecting computer users.

Information security awareness knowledge can be transferred using different techniques. The work conducted in this study used online game play and a training session. The following findings were identified:

- The results from the analysis of the questionnaires showed a decrease in the overall information security awareness levels of the participants. It was expected that the information security awareness levels would have increased, as the work on knowledge retention showed that knowledge would be reinforced by using game play to supplement the training session. Upon further investigation this finding can be attributed to motivation. In other words, the participants lost interest in the information security awareness program after the reward was given to one of the participants as the winner of the game.
- The analysis of online game data showed an increase in the levels of knowledge about information security awareness topics, which contradicts the final findings from the questionnaire results. This could be attributed by the “thin-slicing” effect, as the results showed a decrease in answering time while the response rate increased as the game progressed. The participants wanted to earn more points by answering more questions as the game time expired.

An interesting observation from the data was that participants took consistently less time to answer correctly than to answer incorrectly, even as the response rate increased. This finding could also be supported by the positive effect of reinforcement



of knowledge by repetition of the content within an interval as defined by the spacing effect.

- The effect of the reward on motivation was not considered during the design of the research instrument. The initial idea of the reward was to entice participation to the study and not influence the outcome of the study. Motivation has a substantial impact on the execution of a task. As this study has shown, the impact of rewards and motivation needs to be considered as part of the study design. As a control group was not used during the study, the findings of the effects on motivation cannot be supported by collected data.
- The use of questionnaires to measure knowledge transfer should be used with other metrics to provide a more accurate result. Although several studies use questionnaires to measure the participant's knowledge additional methods should be designed to measure the application of knowledge. For example, the use of an interactive game would have provided a more accurate reflection of knowledge use within a given scenario.

One of the main objectives of the study was to determine if game play has a positive effect on the retention of knowledge transfer. The results from the analysis of the data collected show that game play using reinforcement strategies is conducive to the increase of information security awareness knowledge within a group of participants.

This study is not exhaustive and only looked at a subset of available research tools constrained by limiting factors namely funds and time. The next section concludes this chapter.

## **8.4 Conclusion**

This chapter discussed the implementation of the last phase of the NIST information security awareness framework. The post implementation phase provided a feedback mechanism to improve on the design, development and deployment of an information security awareness program.

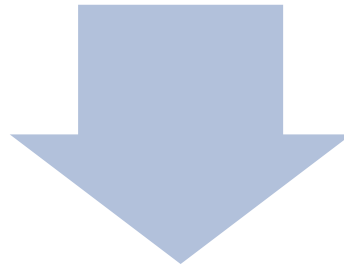
This chapter covered the important components required for data collection (through the use of questionnaires and quizzes) as well as the analysis of the collected data from these instruments. The questionnaires and quizzes were used to assess the information security awareness levels between different transfer platforms which include a training session and

online game play. The findings highlight the impact of reinforcing knowledge through the use of game play as well as the effect of motivation on performance.

The final chapter concludes this dissertation.

## Chapter 9: Conclusion

Chapter 8 - Post Implementation (Analysis of Data)



### Chapter 9 - Conclusion

- 9.1 Introduction
- 9.2 Revisiting the Problem Statement
- 9.3 Main Contribution
- 9.4 Future Work
- 9.5 Publications

Figure 9-1: Layout of Chapter 9

## **9.1 Introduction**

This dissertation addressed the effectiveness of using gaming components as part of an information security awareness program. The motivation for this study was described in Chapter 1. Through the research conducted on the threats targeting the end user, a need for an information security awareness program was identified. In addition, the implementation of an effective mechanism to transfer knowledge, resulting in information security-minded behaviour, was described.

In this dissertation, various mechanisms were analysed. The research subsequently focused on the gaming component, which has been demonstrated as effective in other domains. The analysis of the collected data has also proved that gaming could be effective within the information security awareness domain; however, the effects of extrinsic and intrinsic motivation need to be considered within the design phase of the information security awareness program.

The effectiveness of gaming within an information security awareness program has been explored. Subsequently the importance of this mechanism can be assessed. The process defined within the life cycle of information security awareness programs has been investigated and subsequently one framework was selected for this study. The design, development, implementation and post implementation phases were practically applied with the aim of determining the effectiveness of a gaming component within an information security awareness program.

## **9.2 Revisiting the Problem Statement**

Initial research by the author found many users accessing social networking sites mostly do not adhere to security best practices (Anthonyamy, Greenwood & Rashid 2013). Data collected during preliminary research suggested that a high number of social networking site users unknowingly leak personal information because they do not know how to use privacy controls correctly (Erlandsson, Boldt & Johnson 2012). Sadeghian, Zamani and Shanmugam (2013) also identified additional threats which include but is not limited to spam, phishing, a malicious shortened uniform resource identifier (URL) and fake users. Uninformed users might not even realise this is a threat, and therefore they might not consider information security important. Information security does not form part of these users' reality, resulting in behaviours which could be detrimental to their online safety.

Subsequently, further background information on the current state of cybercrime was obtained through a literature study to support the findings of the initial research (Section 2.3). This identified the need to address threats originating from the Internet that target these uninformed users, to whom we can refer to as 'information security novices', through the development of an information security awareness program.

An understanding of information security awareness programs was achieved by conducting a literature study to formulate the steps required to design, develop, implement and evaluate the effectiveness of an information security awareness program required for this study (Chapter 3).

As a result, the topics affecting information security novices were determined with research conducted on users at Internet Cafés in rural areas in Tshwane (Gauteng, South Africa). Users at Internet Cafés use computers to access resources on the Internet, which include but are not limited to social networking sites, email and content (Section 5.2.1).

Following the identification of the relevant topics (Section 5.2.3), the design and development of the delivery mechanism had to be completed. Many information security awareness delivery mechanisms exist, including posters, email messages and presentations. The use of games to transfer knowledge to users has been observed in many research fields. For example, Lenoir (2003) described the development of games to train military personal in the United States (US) military. The game "*America's Army: Operations*" was developed to identify potential military recruits (Zyda, Mayberry, Wardynski, Shilling & Davis 2003), while flight simulators were developed to train pilots in a simulated environment (Bell & Waag 1998). In the medical field, computer games were also developed to reduce errors during surgeries (Graafland, Schraagen & Schijven 2012).

Many computer games have been developed to be played on several platforms which include personal computers, laptops, mobile devices and the Internet. The use of social networking sites within the Internet domain was selected due to the high adoption rates by users. Several sites provide mechanisms to deploy custom developed applications. The high use of social networking sites together with the development tools provided by these sites resulted in the creation of applications within these platforms (Hui, Lin & Li 2013). These applications focus on a wide variety of ideas which include but are not limited to entertainment and education. For example, IgnitePlay (2011) was developed to promote healthy living with the use of gamification, in other words gain points by performing desired

actions (Yohannis, Prabowo & Waworuntu 2014). Another social networking game developed by Corcoba and Munoz (2013) focus on changing bad driving behaviour. Both these games demonstrate the use of games to change behaviour. Information security awareness also focuses on the adaption of user behaviour. Consequently the objective of the social networking game would be designed around the theme of information security awareness. A literature study was conducted on the design of a game to deliver the selected information security awareness content through social networking sites.

Thereafter, the social networking site game was developed and deployed. The game formed part of the information security awareness program, which also included the development of training material covering the identified topics. Questionnaires were also designed and developed as a qualitative research tool to provide a dataset to determine the effectiveness of the information security awareness program.

In brief, the effectiveness of the information security awareness program could be determined by the data collected during the implementation phase. The data collection process entailed: a pre-assessment using questionnaires to determine the initial information security awareness levels of the participants; presentation of training material which focused on the identified information security topics, then an interim assessment; playing online games on the information security topics, and then another final assessment after the game playing. The data sets were compared to determine if game play could be used to enhance learning the content of information security awareness programs.

To summarise, the focus of this dissertation was to determine the effectiveness of gaming within an information security awareness program. Numerous information security awareness frameworks exist within the information security awareness domain, therefore the selection of the most appropriate framework for the intended audience is critical. Next, an understanding of the life cycle of the selected framework was required to allow customisation and effective implementation. Information security awareness programs can be delivered to the target audience using various mechanisms therefore the need to determine the effectiveness of gaming components as part of information security awareness program arose.

This dissertation aimed to answer the following questions:

**What is the current security knowledge of information security novices?**

An information security awareness program can only be implemented where a need has been identified, otherwise the endeavour would be considered as wasteful expenditure. Considering the number of security breaches disclosed and the end users who have fallen prey to cybercrime the general security knowledge of end users is considered “unsatisfactory” (Section 1.1).

This was supported by research conducted in Section 5.3 on the threats originating from social networking sites, which highlighted the ignorance of end users who have not implemented privacy control correctly.

**What threat categories should be included in an information security awareness program for information security novices?**

A wide variety of threat vectors exist which could be used for nefarious purposes. Many of these threats require the end user to perform an action before exploitation can occur. Also, many of these threats fall outside of the knowledge domain of the novice end user, as in the case of Denial of Service attacks and Zero Day attacks. End users, as discussed within the context of this dissertation, use computer resources on a daily basis to conduct activities. However they do not consider the security concerns of using computers.

A literature study was conducted in Section 5.2.3 to identify which topics should be considered to protect end users. Subsequently a list of information security awareness topics was identified. These in turn could be used to develop information security awareness material to educate the end user resulting in the mitigation of threats.

**How effective are lecture based information security awareness programs?**

As part of the information security awareness program conducted within this study, one of the components was the use of in-person training, also known as lecture based training. This occurred between the pre-assessment (PRE) and the post-assessment (P1). The topics identified in Section 5.4 formed the basis of the lecture. The results from the analysis of the collected data did not indicate that the lecture had a significant impact on the participants (Section 8.2.1). It should also be noted that lecture based training is considered as one-directional communication, transfers knowledge in one direction, and

has limitations, as described in Section 7.3.3. For example, one-directional communication informs an audience but is not designed to promote understanding.

### **How is the effectiveness of an information security awareness program measured?**

The effectiveness of information security awareness programs are measured through changes in behaviour. The observation of the participants' behaviour before and after an information security awareness programs is critical. Information security awareness metrics are useful to collect data from the environment. The testing of information security awareness levels can be achieved by deploying metrics that focus on the testing of knowledge, as in the case of questionnaires.

This dissertation has demonstrated the use of questionnaires to measure the information security awareness levels of the participants (Section 8.2). Due to time and funding this study was limited to only questionnaires; however the effectiveness of future information security awareness programs can be increased by deploying additional metrics.

### **What components are found in an information security awareness program?**

Several information security awareness frameworks exist for the standardisation and implementation of information security awareness programs (Chapter 3). It was noticed that all frameworks have a life cycle represented by phases which each one need to be completed before moving to the next phase. A needs assessment and topic identification were conducted in the design phase (Chapter 5). The development phase described the platform to be used to deliver the content to the target audience (Chapter 6). During the implementation phase, the information security awareness program was deployed to the target audience and also collected data from the participants (Chapter 7). The last phase analysed the data collected during the information security awareness program; the findings subsequently to be used to improve the information security awareness program (Chapter 8).

It is imperative to consider the impact of the platforms used to deliver the content of the information security awareness. The learning styles of the participants, environment, costs and time are identified constraints that impact the implementation of an information security awareness program. These affect the impact the information security awareness program has on the participants as seen by the impact of motivation.



## **How effective are games as a platform to deliver information security awareness?**

The main focus of the dissertation was to determine the effectiveness of gaming components as part of an information security awareness program. The analysis of the data collected during the game play supported the notion that gaming does have a positive effect by increasing knowledge retention and learning (Chapter 8).

A holistic view of the collected data from the assessments indicated an event which affected the results. Upon investigation, the effect of intrinsic and extrinsic motivation was identified as the cause of the negative result. Subsequently the impact of the game as part of the information security awareness program is inconclusive as the last assessment results were skewed. Also, the data collected during the game play tracked individual performance, but this data cannot be linked to an individual's assessment data, resulting in unreliable conclusions as described in Section 8.3.

### **9.3 Main Contribution**

This dissertation aimed to contribute in various ways within the domain of information security awareness. A summary of the main contributions is provided:

- The effectiveness of games as part of information security awareness programs has been demonstrated. The game was designed to allow the user to progress based on their interaction with the game. The use of fully interactive and real-time game design improved effectiveness.
- The assessment of knowledge through the use of questionnaires has demonstrated that a correlation exists between a user's response time and the successful answering of the question. In other words, a user takes longer to answer a question if they do not know the answer.
- The effects of intrinsic and extrinsic motivation have been highlighted in this dissertation. Rewards were initially included to entice people to participate in the study – numerous research undertakings use rewards to increase the sample size – however this study has demonstrated the importance of taking human nature into consideration.
- The design of the autonomous information security awareness platform, which could be beneficial to institutions and individuals who do not otherwise have access to these programs due to lack of funding or infrastructure, as seen within rural areas. The autonomous system can effectively monitor the security behaviour, assess the

information security awareness levels of a group, conduct information security awareness training and manage Internet access.

- A list of information security awareness topics which affect end users who do not have an information security background. The identification of different methods used to target end users would improve the effectiveness of information security awareness programs, as the topics focus on what is relevant to these users.

## 9.4 Future Work

On the basis of these findings, future work would address the following:

- The development and deployment of the autonomous information security awareness system will be addressed in future. The focus of this dissertation was the identification of a gaming component and measuring its effectiveness. This forms part of the information security awareness metrics required to measure the awareness levels within an establishment. With this component completed, the focus needs to be moved toward the development of a high level system to automate the process of information security awareness at remote locations.
- The game design should be transformed into a fully interactive game which resembles a quest. The use of a quest is synonymous with applying knowledge to encountered situations. In the domain of information security awareness, the quest could be to instil good security practices, as in the case of password management or when transporting computer equipment.
- A critical component which was not addressed in this dissertation is the customisation of the content to align with the learning style of the individual. In other words, to create content based on the personality of the user which by design would be better understood, resulting in longer retention of the knowledge.
- Webb, Ahmad, Maynard and Shanks (2014) provided evidence that personality influences the effectiveness of information security awareness messages. The use of personalised security messages could be added to the information security awareness metrics. The design principles must be investigated to be able to develop a system. Subsequently this system should profile the users and automatically create information security awareness material based on personality.

## 9.5 Publications

As proof of the contribution this study has made to the information security awareness body of knowledge, the following papers were presented and published in peer-reviewed conference proceedings. Copies of these papers can be found in Appendix G.

- Labuschagne, W.A. & Eloff, M.M. 2014, "The Effectiveness of Online Gaming as Part of a Security Awareness Program", 13th European Conference on Cyber Warfare and Security (ECCWS), Academic Conferences Limited, Reading, United Kingdom, 3 - 4 July 2014, pp. 125-132.
- Veerasamy, N. & Labuschagne, W.A. 2014, "Determination of Meme Proliferation Factors", 13th European Conference on Cyber Warfare and Security (ECCWS), Academic Conferences Limited, Reading, United Kingdom, 3 - 4 July 2014, pp. 188-197.
- Labuschagne, W.A., Veerasamy, N. & Eloff, M.M. 2013, "Dangers of Social Networking Sites - the Propagation of Malware", 12th European Conference on Cyber Warfare and Security (ECCWS), Academic Conferences Limited, Reading, United Kingdom, 11 - 12 July 2013, pp. 173-181.
- Labuschagne, W.A. & Eloff, M.M. 2012, "Towards an automated security awareness system in a virtualized environment", 11th European Conference on Information Warfare and Security (ECIW), Academic Conferences Limited, Reading, United Kingdom, 5 - 6 July 2012, pp. 163-171.
- Labuschagne, W.A., Eloff, M.M. & Veerasamy, N. 2012, "The dark side of Web 2.0", 10th IFIP TC 9 International Conference on Human Choice and Computers (HCC10), Springer, Berlin, Germany, 27 - 28 September 2012, pp. 237-249.
- Labuschagne, W.A., Eloff, M.M., Veerasamy, N., Leenen, L. & Mujinga, M. 2011, "Design of a Cyber Security Awareness Campaign for Internet Cafe Users in Rural Areas", Proceedings of the first IFIP TC9 / TC11 Southern African Cyber Security Awareness Workshop (SACSAW), Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa, 12 May 2011, pp. 42-59.
- Labuschagne, W.A., Veerasamy, N., Burke, I. & Eloff, M.M. 2011, "Design of cyber security awareness game utilizing a social media framework", Proceedings of the Information Security South Africa (ISSA), IEEE, New Jersey, United States of America, 15 - 17 August 2011, pp. 175-183.

## 10 References

- Abraham, S. & Chengalur-Smith, I. 2010, "An overview of social engineering malware: Trends, tactics, and implications", *Technology in Society*, vol. 32, no. 3, pp. 183-196.
- Albrechtsen, E. & Hovden, J. 2010, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers & Security*, vol. 29, no. 4, pp. 432-445.
- Allodi, L., Corradin, M. & Massacci, F. 2015, "Then and now: on the maturity of the cybercrime markets (The lesson that black-hat marketeers learned)", *IEEE Transactions on Emerging Topics in Computing*, vol. 2168-6750, no. 99, pp. 1-11.
- Ambady, N. & Rosenthal, R. 1992, "Thin slices of expressive behavior as predictors of interpersonal consequences: A meta-analysis", *Psychological bulletin*, vol. 111, no. 2, pp. 256-274.
- Anselmi, D. & Boscovich, R. 2010, *Microsoft Security Intelligence Report 2010*, Microsoft, Washington, United States of America, Available: [http://download.microsoft.com/download/6/0/5/605BE103-9429-4493-898B-E3D50AB68236/Microsoft\\_Security\\_Intelligence\\_Report\\_volume\\_10\\_July-Dec2010\\_English.pdf](http://download.microsoft.com/download/6/0/5/605BE103-9429-4493-898B-E3D50AB68236/Microsoft_Security_Intelligence_Report_volume_10_July-Dec2010_English.pdf).
- Anthonyamy, P., Greenwood, P. & Rashid, A. 2013, "Social Networking Privacy: Understanding the Disconnect from Policy to Controls", *IEEE Computer Society*, vol. 46, no. 6, pp. 60-67.
- AV-TEST 2015, March 25 - last update, *Malware* [Homepage of AV-TEST], [Online]. Available: <http://www.av-test.org/en/statistics/malware/> [Accessed: 2015, March 25].
- Awan, R.R. 2007, *EasyHotspot*, 0.2nd edn, EasyHotspot, Jakarta, Indonesia.
- Baggett, M. 2008, *Effectiveness of Antivirus in Detecting Metasploit Payloads*, SANS Institute, Swansea, United Kingdom, Available: [http://www.sans.org/reading\\_room/whitepapers/casestudies/effectiveness-antivirus-detecting-metasploit-payloads\\_2134](http://www.sans.org/reading_room/whitepapers/casestudies/effectiveness-antivirus-detecting-metasploit-payloads_2134).
- Balnaves, M. & Caputi, P. 2001, *Introduction to quantitative research methods: An investigative approach*, 1st edn, SAGE Publications Ltd, California, United States of America.
- Barlowe, B. & Blackbird, J. 2012, *The evolution of malware and the threat landscape - a 10 - year review*, Microsoft Corporation, Redmond, United States of America, Available: <http://www.microsoft.com/en-us/download/details.aspx?id=29046>.
- Barnes, N.D. & Barnes, F.R. 2009, "Equipping your organization for the social networking game", *Information Management*, vol. 43, no. 6, pp. 28-33.
- Barrett, N. 2003, "Penetration testing and social engineering: Hacking the weakest link", *Information Security Technical Report*, vol. 8, no. 4, pp. 56-64.
- Barth, A., Felt, A.P., Saxena, P. & Boodman, A. 2010, "Protecting Browsers from Extension Vulnerabilities", *NDSS*, The Internet Society, Geneva, Switzerland, 28 February - 3 March 2010, pp. 1-13.
- Beaver, K. (ed) 2007, *Hacking for dummies*, 2nd edn, Wiley Publishing Inc., Indiana, United States of America.
- Bell, D.S., Harless, C.E., Higa, J.K. & Mangione, C.M. 2008, "Knowledge retention after an online tutorial: A randomized educational experiment among resident physicians", *Journal of general internal medicine*, vol. 23, no. 8, pp. 1164-1171.
- Bell, H.H. & Waag, W.L. 1998, "Evaluating the effectiveness of flight simulators for training combat skills: A review", *The international journal of aviation psychology*, vol. 8, no. 3, pp. 223-242.
- Bell, M. & Lintumaa, K. 2011, *Virtual Machines: Added planning to the forensic acquisition process*, 29th edn, (In)Secure, Greenwood Village, United States of America.
- Bilge, L. & Dumitras, T. 2012, "Before we knew it: an empirical study of zero-day attacks in the real world", *Proceedings of the 2012 ACM conference on Computer and communications security*, Association for Computing Machinery, New York, United States of America, 16 - 18 October 2012, pp. 833-844.
- Birnhack, M.D. 2008, "The EU Data Protection Directive: An engine of a global regime", *Computer Law & Security Review*, vol. 24, no. 6, pp. 508-520.

- Britz, M.T. 2009, *Computer Forensics and Cyber Crime: An Introduction*, 2nd edn, Pearson Education India, Delhi, India.
- Brodie, R. 2011, *Virus of the Mind: The New Science of the Meme*, 1st edn, Hay House, Carlsbad, United States of America.
- Bryman, A. & Bell, E. 2011, *Business Research Methods*, 3rd edn, Oxford University Press, Oxford, United Kingdom.
- Cavalca, D. & Goldoni, E. 2008, "HIVE: an Open Infrastructure for Malware Collection and Analysis", *1st Workshop On Open Source Software For Computer And Network Forensics*, OSSCoNF, Milan, Italy, 7 - 10 September 2008, pp. 23-34.
- Chai, B. 2011, April 19 - last update, *Firewalls, Only 60 Per Cent Effective Against Malware* [Homepage of ITProPortal], [Online]. Available: <http://www.itproportal.com/2011/04/19/firewalls-only-60-cent-effective-against-malware/> [Accessed: 2012, December 18].
- Chen, H. 2012, *Dark web: Exploring and data mining the dark side of the web*, 1st edn, Springer-Verlag, New York, United States of America.
- Chen, Y., Boehm, B. & Sheppard, L. 2007, "Value driven security threat modeling based on attack path analysis", *40th Annual Hawaii International Conference on System Sciences*, IEEE, New Jersey, United States of America, 3 - 6 January 2007, pp. 280-289.
- Chou, C. & Peng, H. 2011, "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience", *The Internet and Higher Education*, vol. 14, no. 1, pp. 44-53.
- Chuttur, M. 2009, "Overview of the technology acceptance model: Origins, developments and future directions", *Sprouts: Working Papers on Information Systems*, vol. 9, no. 37, pp. 1-23.
- Cialdini, R.B. 1998, *Influence: The Psychology of Persuasion*, 2nd edn, Collins, New York, United States of America.
- Ciampa, M. 2004, *Security Guide to Networking Security Fundamentals*, 2nd edn, Course Technology Press, Boston, United States of America.
- Cohn, M.A., Mehl, M.R. & Pennebaker, J.W. 2004, "Linguistic markers of psychological change surrounding September 11, 2001", *Psychological Science*, vol. 15, no. 10, pp. 687-693.
- Colón, M. 2014, June 16 - last update, *"Human error" contributes to nearly all cyber incidents, study finds* [Homepage of Haymarket Media, Inc], [Online]. Available: <http://www.scmagazine.com/human-error-contributes-to-nearly-all-cyber-incidents-study-finds/article/356015/> [Accessed: 2014, November 23].
- Cone, B.D., Irvine, C.E., Thompson, M.F. & Nguyen, T.D. 2007, "A video game for cyber security training and awareness", *Computers & Security*, vol. 26, no. 1, pp. 63-72.
- Constantin, L. 2014, September 2 - last update, *Hackers make drive-by download attacks stealthier with fileless infections*. [Homepage of IDG Consumer & SMB], [Online]. Available: <http://www.pcworld.com/article/2601140/hackers-make-driveby-download-attacks-stealthier-with-fileless-infections.html> [Accessed: 2014, October 23].
- Coppens, B., De Sutter, B. & De Bosschere, K. 2013, "Protecting Your Software Updates", *Security Privacy, IEEE*, vol. 11, no. 2, pp. 47-54.
- Corcoba Magaña, V. & Muñoz Organero, M. 2013, "GAFU: A game to save fuel using social networks", *International Conference on Connected Vehicles and Expo (ICCVEx)*, IEEE, New Jersey, United States of America, 2 - 6 December 2013, pp. 151-157.
- Cramer, D. 2011, October 24 - last update, *Computer security phone scam hits SA* [Homepage of Mybroadband], [Online]. Available: <http://mybroadband.co.za/news/security/36722-computer-security-phone-scam-hits-sa.html> [Accessed: 2012, April 13].
- Cricket, L. 2013, October 30 - last update, *The ultimate guide to preventing DNS-based DDoS attacks* [Homepage of Infoworld], [Online]. Available: <http://www.infoworld.com/t/security/the-ultimate-guide-preventing-dns-based-ddos-attacks-229790> [Accessed: 2014, May 24].
- Csikszentmihalyi, M. 1991, *Flow: The Psychology of Optimal Experience*, 1st edn, Harper Perennial, New York, United States of America.

- Davis, L., Holden, D., Jagdale, P., Gragido, W., Hein, B. & Hils, A. 2011, *2011 Top cyber security risks report*, Hewlett-Packard Development Company, California, United States of America, Available: <http://www.websense.com/assets/reports/report-2012-threat-report-en.pdf>.
- Davis, F.D. 1985, *A technology acceptance model for empirically testing new end-user information systems: theory and results*, Massachusetts Institute of Technology.
- De la Rouviere, N. 2012, January 30 - last update, *How To: Learn Better by Learning Less* [Homepage of MIH Media Lab], [Online]. Available: <http://ml.sun.ac.za/2012/01/30/how-to-learn-better-by-learning-less> [Accessed: 2013, September 23].
- Deci, E.L. 1971, "Effects of externally mediated rewards on intrinsic motivation", *Journal of personality and social psychology*, vol. 18, no. 1, pp. 105-115.
- Department of Defence (United States of America) 1999, *CyberProtect*, 1st edn, Defense Information Systems Agency, Carney, United States of America.
- Dey, I. 2003, *Qualitative data analysis: A user friendly guide for social scientists*, 1st edn, Routledge, London, United Kingdom.
- Dictionary.com 2012a, April 19 - last update, *Dictionary.com's 21st Century Lexicon (CyberCrime)* [Homepage of Dictionary.com], [Online]. Available: <http://dictionary.reference.com/browse/cybercrime> [Accessed: 2012, April 19].
- Dictionary.com 2012b, April 19 - last update, *Dictionary.com's 21st Century Lexicon (Protection)* [Homepage of Dictionary.com], [Online]. Available: <http://dictionary.reference.com/browse/protection> [Accessed: 2012, April 19].
- Dictionary.com 2012c, April 20 - last update, *The Free On-line Dictionary of Computing (Security)* [Homepage of Dictionary.com], [Online]. Available: <http://dictionary.reference.com/browse/security> [Accessed: 2012, April 20].
- Dodge, R.C. 2007, "Phishing for user security awareness", *Computers & Security*, vol. 26, no. 1, pp. 73-80.
- Dougiamas, M. 1999, *Modular Object-Oriented Dynamic Learning Environment*, 2.1.2 edn, Moodle Pty Ltd, Perth, Australia.
- Dretzke, B.J. 2005, *Statistics with Microsoft Excel*, 5th edn, Pearson, London, United Kingdom.
- Du Zhang, Jujjavarapu, L. & Meiliu Lu 2014, "Detecting and resolving inconsistencies in firewalls", *IEEE 15th International Conference on Information Reuse and Integration (IRI)*, IEEE, New Jersey, United States of America, 13 - 15 August 2014, pp. 1-7.
- Duebendorfer, T. & Frei, S. 2009, *Why silent updates boost security*, ETH Zurich, Zurich, Germany, Available: <http://www.techzoom.net/publications/silent-updates>.
- Dutta, A. & McCrohan, K. 2002, "Management's role in information security in a cyber economy", *California management review*, vol. 45, no. 1, pp. 67-87.
- Dwyer III, S.J., Weaver, A.C. & Hughes, K.K. 2004, "Health Insurance Portability and Accountability Act", *Security Issues in the Digital Medical Enterprise*, vol. 72, no. 2, pp. 9-18.
- El Kharbili, M., Stein, S., Markovic, I. & Pulvermüller, E. 2008, "Towards a framework for semantic business process compliance management", *Proceedings of the workshop on Governance, Risk and Compliance for Information Systems*, Springer-Verlag, Berlin, Germany, 16 - 20 June 2008, pp. 1-15.
- El-Nasr, M.S., Andres, L., Lavender, T., Funk, N., Jahangiri, N. & Mengting Sun 2011, "IgnitePlay: Encouraging and sustaining healthy living through social games", *Games Innovation Conference (IGIC)*, IEEE, New Jersey, United States of America, 2 - 3 November 2011, pp. 23-25.
- Eminağaoğlu, M., Uçar, E. & Eren, Ş. 2009, "The positive outcomes of information security awareness training in companies - A case study", *Information Security Technical Report*, vol. 14, no. 4, pp. 223-229.
- Enders, A., Hungenberg, H., Denker, H. & Mauch, S. 2008, "The long tail of social networking: Revenue models of social networking sites", *European Management Journal*, vol. 26, no. 3, pp. 199-211.
- England, P. & Manfredelli, J. 2006, "Virtual machines for enterprise desktop security", *Information Security Technical Report*, vol. 11, no. 4, pp. 193-202.



- ENISA 2010, *The new users' guide: How to raise information security awareness*, European Network and Information Security Agency (ENISA), Athens, Greece, Available: [http://www.enisa.europa.eu/publications/archive/copy\\_of\\_new-users-guide/at\\_download/fullReport](http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport).
- En-Najjary, T. & Urvoy-Keller, G. 2010, "A first look at traffic classification in enterprise networks", *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, ACM, New York, United States of America, 23 - 25 September 2010, pp. 764 - 768.
- Erlandsson, F., Boldt, M. & Johnson, H. 2012, "Privacy Threats Related to User Profiling in Online Social Networks", *International Conference on Privacy, Security, Risk and Trust (PASSAT) and International Conference on Social Computing (SocialCom)*, IEEE, New Jersey, United States of America, 3 - 5 September 2012, pp. 838-842.
- Evans, D.C., Gosling, S.D. & Carroll, A. 2008, "What elements of an online social networking profile predict target-rater agreement in personality impressions", *Proceedings of the International Conference on Weblogs and Social Media*, The AAAI Press, California, United States of America, 30 March – 2 April 2008, pp. 1-6.
- Evans, J.R. & Mathur, A. 2005, "The value of online surveys", *Internet Research*, vol. 15, no. 2, pp. 195-219.
- Evans, J. 2011, *The Social Web Threat*, 01/2011(37) edn, Hakin9 Media, Warszawa, Poland.
- Evans, J. 2010, *A Brief Analysis of the Cyber Security Threat*, 11/2010(36) edn, Haking9 Media, Warszawa, Poland.
- Felder, R.M. & Silverman, L.K. 1988, "Learning and teaching styles in engineering education", *Engineering Education*, vol. 78, no. 7, pp. 674-681.
- Fiedler, K. 2007, "The psychological function of function words" in *Social Communication (Frontiers of Social Psychology)*, 1st edn, Psychology Press New York, New York, United States of America, pp. 343-359.
- FireEye 2012, *FireEye Advanced Threat Report – 1H 2012*, FireEye Inc, California, United States of America, Available: <http://www2.fireeye.com/advanced-threat-report-1h2012.html>.
- Fogarty, K. 2011, April 13 - last update, *Tests show reputation of firewall's effectiveness 'grossly overstated'* [Homepage of IT World], [Online]. Available: <http://www.itworld.com/security/155717/tests-show-reputation-firewalls-effectiveness-grossly-overstated> [Accessed: 2012, December 17].
- Forouzan, B.A. 2003, "Hypertext Transfer Protocol" in *TCP/IP Protocol Suite*, 2nd edn, McGrawHill, New York, United States, pp. 649-663.
- Frei, S., Tellenbach, B. & Plattner, B. 2008, *0-Day patch exposing vendors (in) security performance*, BlackHat Europe edn, Blackhat, Amsterdam, Netherlands.
- Fung, C.C., Khera, V., Depickere, A., Tantatsanawong, P. & Boonbrahm, P. 2008, "Raising information security awareness in digital ecosystem with games-a pilot study in Thailand", *2nd IEEE International Conference on Digital Ecosystems and Technologies*, IEEE, New Jersey, United States of America, 26 - 29 February 2008, pp. 375-380.
- Furuholt, B., Kristiansen, S. & Wahid, F. 2008, "Gaming or gaining? Comparing the use of Internet cafés in Indonesia and Tanzania", *The International Information & Library Review*, vol. 40, no. 2, pp. 129-139.
- Gollmann, D. 2010, "Computer security", *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 2, no. 5, pp. 544-554.
- Goodin, D. 2012, October 16 - last update, *Zero-day attacks are meaner, more rampant than we ever thought* [Homepage of Arstechnic], [Online]. Available: <http://arstechnica.com/security/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought/> [Accessed: 2013, January 03].
- Goodman, S.E., Kirk, J.C. & Kirk, M.H. 2007, "Cyberspace as a medium for terrorists", *Technological Forecasting and Social Change*, vol. 74, no. 2, pp. 193-210.
- Google Code Lab 2015, March 18 - last update, *Google Safe Browsing* [Homepage of Google Inc], [Online]. Available: <http://code.google.com/apis/safebrowsing/> [Accessed: 2012, March 06].
- Google Inc 2014, May 24 - last update, *So much time, so little spam* [Homepage of Google Inc], [Online]. Available: <https://www.gmail.com/intl/en/mail/help/fightspam/spamexplained.html> [Accessed: 2014, May 24].
- Graafland, M., Schraagen, J. & Schijven, M. 2012, "Systematic review of serious games for medical education and surgical skills training", *British journal of surgery*, vol. 99, no. 10, pp. 1322-1330.

- Graham-Cumming, J. 2014, September 30 - last update, *Inside Shellshock: How hackers are using it to exploit systems* [Homepage of Cloudflare], [Online]. Available: <http://blog.cloudflare.com/inside-shellshock/> [Accessed: 2014, October 28].
- Grandjean, E. 2008, "A prime target for social engineering malware", *McAfee Security Journal*, vol. Security Vision, no. Fall 2008, pp. 16-22.
- Gregory, M.A. & Glance, D. 2013, "Predictions" in *Security and the Networked Society*, 1st edn, Springer, Berlin, Germany, pp. 289-297.
- Haffejee, J. & Irwin, B. 2014, "Testing antivirus engines to determine their effectiveness as a security layer", *Information Security for South Africa (ISSA)*, IEEE, New Jersey, United States of America, 13 - 14 Augustus 2014, pp. 1-6.
- Harlan, C. 2005, "Malware analysis for windows administrators", *Digital Investigation*, vol. 2, no. 1, pp. 19-22.
- Harris, S. 2005, *All in one CISSP exam guide*, 3rd edn, McGraw-Hill/Osborne, New York, United States of America.
- Hirsh, J.B. & Peterson, J.B. 2009, "Personality and language use in self-narratives", *Journal of Research in Personality*, vol. 43, no. 3, pp. 524-527.
- Hobbs, J. & Bristow, T. 2007, "Communal computing and shared spaces of usage: a study of Internet cafes in developing contexts", *IA Summit*, Journal of the Association for Information Science and Technology, Maryland, United States of America, 22 - 26 March 2007, pp. 1-12.
- Hsu, C.L. & Lu, H.P. 2004, "Why do people play on-line games? An extended TAM with social influences and flow experience", *Information & Management*, vol. 41, no. 7, pp. 853-868.
- Hui, L., Lin, W. & Li, X. 2013, "A study of integrating social networking service into the virtual pet web game system", *International Joint Conference on Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA)*, IEEE, New Jersey, United States of America, 2 - 4 November 2013, pp. 412-418.
- Huizenga, J., Admiraal, W., Akkerman, S. & ten Dam, G. 2009, "Cognitive and affective effects of learning History by playing a mobile game", *Proceedings of the 2nd European Conference on Games-Based Learning*, Academic Conferences and Publishing International Limited, Reading, United Kingdom, 16 - 17 October 2008, pp. 207-212.
- Hulitt, E. & Vaughn, R.B. 2010, "Information system security compliance to FISMA standard: a quantitative measure", *Telecommunication Systems*, vol. 45, no. 2-3, pp. 139-152.
- Humphreys, E. 2007, *Implementing the ISO/IEC 27001 information security management system standard*, 1st edn, Artech House, Inc., Boston, United States of America.
- Hyde-Clark, N. 2006, "The Urban Digital Divide: A Comparative Analysis of Internet Cafés in Johannesburg, South Africa", *Review of African Political Economy*, vol. 33, no. 107, pp. 150-156.
- Ikinci, A., Holz, T. & Freiling, F. 2008, "Monkey-spider: Detecting malicious websites with low-interaction honeyclients", *Proceedings of Sicherheit, Schutz und Zuverlässigkeit*, vol. 8, pp. 407-421.
- Imperva 2012, *Assessing the Effectiveness of Antivirus Solutions*, Hacker Intelligence Initiative, California, United States, Available: [http://www.imperva.com/docs/HII\\_Assessing\\_the\\_Effectiveness\\_of\\_Antivirus\\_Solutions.pdf](http://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf).
- International Standards Organisation 2012, *Information technology - Security techniques - Guidelines for cybersecurity*, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), New York, United States of America, Available: <http://www.iso27001security.com/html/27032.html>.
- Jaquith, A. 2007, *Security metrics: replacing fear, uncertainty, and doubt*, 1st edn, Addison-Wesley Upper Saddle River, New Jersey, United States of America.
- Joe, S. 2004, "This business of malware", *Information Security Technical Report*, vol. 9, no. 2, pp. 35-41.
- Johnston, J., Eloff, J.H.P. & Labuschagne, L. 2003, "Security and human computer interfaces", *Computers & Security*, vol. 22, no. 8, pp. 675-684.
- Judson, D.H. 1996, "Web browser with dynamic display of information objects during linking", *Web browser with dynamic display of information objects during linking*, .



- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), 7:1-7:31.
- Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, San Jose, California, USA. pp. 905-914.
- Kaspersky Lab 2014, January 14 - last update, "Red October" Diplomatic Cyber Attacks Investigation [Homepage of Kaspersky Lab ZAO], [Online]. Available: <http://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/> [Accessed: 2014, November 23].
- Kennedy, D., O'Gorman, J., Kearns, D. & Aharoni, M. 2011, *Metasploit: The Penetration Tester's Guide*, 1st edn, No Starch Press, San Francisco, United States of America.
- Khan, B., Alghathbar, K.S., Nabi, S.I. & Khan, M.K. 2011, "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, vol. 5, no. 26, pp. 10862-10868.
- Khan, S. 2011, *Let's use video to reinvent education*, 1st edn, TED Conferences, LLC, Long Beach, United States of America.
- Kim, W., Jeong, O., Kim, C. & So, J. 2011, "The dark side of the Internet: Attacks, costs and responses", *Information Systems*, vol. 36, no. 3, pp. 675-705.
- Kitchin, R. 1998, *Cyberspace: The world in the wires*, 1st edn, John Wiley & Sons, Inc., New Jersey, United States of America.
- Kolb, A.Y. & Kolb, D.A. 2005, "Learning styles and learning spaces: Enhancing experiential learning in higher education", *Academy of management learning & education*, vol. 4, no. 2, pp. 193-212.
- Kolb, D.A. 1984, *Experiential learning: experience as the source of learning and development*, 1st edn, Prentice Hall, New Jersey, United States of America.
- Kritzinger, E. & von Solms, S.H. 2010, "Cyber security for home users: A new way of protection through awareness enforcement", *Computers & Security*, vol. 29, no. 8, pp. 840-847.
- Kruger, H. & Kearney, W. 2005, "Measuring Information Security Awareness", *Information South Africa (ISSA) Conference*, ISSA, Johannesburg, South Africa, 29 June - 1 July 2005, pp. 1-10.
- Kruger, H.A. & Kearney, W.D. 2006, "A prototype for assessing information security awareness", *Computers & Security*, vol. 25, no. 4, pp. 289-296.
- Kruglanski, A.W., Friedman, I. & Zeevi, G. 1971, "The effects of extrinsic incentive on some qualitative aspects of task performance", *Journal of personality*, vol. 39, no. 4, pp. 606-617.
- Landwehr, C.E. 2001, "Computer security", *International Journal of Information Security*, vol. 1, no. 1, pp. 3-13.
- Lenoir, T. 2003, "Programming theatres of war: Gamemakers as soldiers" in *Bytes, Bandwidth, and Bullets: The emerging relationship between information technology and security*, 1st edn, The New Press, New York, United States of America, pp. 1-22.
- Libicki, M.C. 1995, *What is information warfare?*, National Defense University Washington DC Institute For National Strategic Studies, Washington, United States of America, Available: <http://www.dtic.mil/dtic/tr/fulltext/u2/a367662.pdf>.
- Liszkiewicz, A.J.P. 2010, March 09 - last update, *Cultivated Play: Farmville* [Homepage of Mediacommons], [Online]. Available: <http://mediacommons.futureofthebook.org/content/cultivated-play-farmville> [Accessed: 2013, February 02].
- Madden, M., Fox, S., Smith, A. & Vitak, J. 2007, *Digital Footprints: Online identity management and search in the age of transparency*, Pew Internet & American Life Project, Washington, United States of America, Available: [http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP\\_Digital\\_Footprints.pdf.pdf](http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf).
- Major, C.H. & Savin-Baden, M. 2013, *Qualitative Research: The Essential Guide to Theory and Practice*, 1st edn, Routledge.

- Mann, M.F. & Hill, T. 1984, "Persuasive communications and the boomerang effect: some limiting conditions to the effectiveness of positive influence attempts", *Advances in Consumer Research*, vol. 11, no. 1, pp. 66-70.
- Manning, R. 2010, *Phishing Activity Trends Report*, Anti Phishing Work Group, Jacksonville, United States of America, Available: [http://www.apwg.com/reports/apwg\\_report\\_q2\\_2010.pdf](http://www.apwg.com/reports/apwg_report_q2_2010.pdf).
- Mano, M.M. 1993, *Computer system architecture*, 3rd edn, Prentice Hall, New Jersey, United States of America.
- McCoy, C. & Fowler, R.T. 2004, "You are the key to security: establishing a successful security awareness program", *Proceedings of the 32nd annual ACM SIGUCCS fall conference*, ACM, New York, United States of America, 10 - 13 October 2004, pp. 346-349.
- McDonald, H. 2013, October 30 - last update, *Online fraud costs global economy 'many times more than \$100bn'* [Homepage of The Guardian], [Online]. Available: <http://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars> [Accessed: 2015, February 26].
- McDonald, H. & Adam, S. 2003, "A comparison of online and postal data collection methods in marketing research", *Marketing Intelligence & Planning*, vol. 21, no. 2, pp. 85-95.
- McGill, R., Tukey, J.W. & Larsen, W.A. 1978, "Variations of box plots", *The American Statistician*, vol. 32, no. 1, pp. 12-16.
- McKenney, J. 2011, *Malware: New Capabilities & Directions*, Daily Safety Check, Missouri, United States of America, Available: [http://www.dailysafetycheck.com/v/vspfiles/WhitePaper\\_2012\\_Botnet.pdf](http://www.dailysafetycheck.com/v/vspfiles/WhitePaper_2012_Botnet.pdf).
- Menon, A. & Gabriely, M.G. 2010, *State of the Internet 2010: A Report on the Ever Changing Threat Landscape*, CA Technologies, New York, United States of America, Available: [http://www.ca.com/files/SecurityAdvisorNews/h12010threatreport\\_244199.pdf](http://www.ca.com/files/SecurityAdvisorNews/h12010threatreport_244199.pdf).
- Merriam-Webster 2014a, March 19 - last update, "Framework" [Homepage of Merriam-Webster.com], [Online]. Available: <http://www.merriam-webster.com/dictionary/framework> [Accessed: 2014, March 18].
- Merriam-Webster 2014b, March 19 - last update, "Road Map" [Homepage of Merriam-Webster.com], [Online]. Available: <http://www.merriam-webster.com/dictionary/roadmap> [Accessed: 2014, March 19].
- Microsoft 2014a, June 11 - last update, *MEDIAN function* [Homepage of Microsoft], [Online]. Available: <http://office.microsoft.com/en-za/sharepoint-foundation-help/median-function-HA010379994.aspx?CTT=1> [Accessed: 2014, June 11].
- Microsoft 2014b, June 12 - last update, *STDEVP* [Homepage of Microsoft], [Online]. Available: <http://office.microsoft.com/en-za/excel-help/stdevp-HP005209281.aspx> [Accessed: 2014, June 12].
- Microsoft 2014c, June 11 - last update, *TRIMMEAN* [Homepage of Microsoft], [Online]. Available: <http://office.microsoft.com/en-za/excel-help/trimmean-HP005209322.aspx> [Accessed: 2014, June 11].
- Microsoft 2014d, June 12 - last update, *VARP function* [Homepage of Microsoft], [Online]. Available: <http://office.microsoft.com/en-za/windows-sharepoint-services-help/varp-function-HA001161096.aspx?CTT=1> [Accessed: 2014, June 12].
- Miliefsky, G.S. 2011, *Cybercrime and Cyberwar Predictions for 2011*, 1/2011(37) edn, Hakin9, Warszawa, Poland.
- Miller, J. 2013, August 27 - last update, *Facebook to compensate users for sharing details on ads* [Homepage of BBC News], [Online]. Available: <http://www.bbc.co.uk/news/technology-23848323> [Accessed: 2013, September 12].
- Mirkovic, J. & Reiher, P. 2004, "A taxonomy of DDoS attack and DDoS defense mechanisms", *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53.
- Mohr, G., Kimpton, M., Stack, M. & Ranitovic, I. 2004, "Introduction to Heritrix an archival quality web crawler", *Proceedings of the 4th International Web Archiving Workshop (IWAW'04)*, Springer, Berlin, Germany, 16 September 2004, pp. 1 -15.
- Moon, J.W. & Kim, Y.G. 2001, "Extending the TAM for a World-Wide-Web context", *Information & Management*, vol. 38, no. 4, pp. 217-230.

- Morse, E.A. & Raval, V. 2008, "PCI DSS: Payment card industry data security standards in context", *Computer Law & Security Review*, vol. 24, no. 6, pp. 540-554.
- Nachreiner, C. 2015, March 19 - last update, *Signature antivirus' dirty little secret* [Homepage of Net-Security], [Online]. Available: <http://www.net-security.org/article.php?id=2239> [Accessed: 2015, March 19].
- Nascimento, G. & Correia, M. 2011, "Anomaly-based Intrusion Detection in Software as a Service", *41st International Conference on Dependable Systems and Networks Workshops (DSN-W)*, IEEE Computer Society, Hong Kong, 27 - 30 June 2011, pp. 19-24.
- Naval Postgraduate School & Rivermind, I. 2004, *CyberCIEGE Educational Video Game*, 1st edn, Naval Postgraduate School, California, United States of America.
- Newman, M.L., Groom, C.J., Handelman, L.D. & Pennebaker, J.W. 2008, "Gender differences in language use: An analysis of 14,000 text samples", *Discourse Processes*, vol. 45, no. 3, pp. 211-236.
- Newman, M.L., Pennebaker, J.W., Berry, D.S. & Richards, J.M. 2003, "Lying words: Predicting deception from linguistic styles", *Personality and Social Psychology Bulletin*, vol. 29, no. 5, pp. 665-675.
- Nielsen, J. 2005, *10 Heuristics for User Interface Design*, Nielsen Norman Group, Fremont, United States of America, Available: <http://www.nngroup.com/articles/ten-usability-heuristics/>.
- Nykodym, N., Taylor, R. & Vilela, J. 2005, "Criminal profiling and insider cyber crime", *Digital Investigation*, vol. 2, no. 4, pp. 261-267.
- O'Gorman, G. & McDonald, G. 2012, *Ransomware: a growing menace*, Symantec Corporation, Mountain View, United States of America, Available: [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/ransomware-a-growing-menace.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf).
- Opdenakker, R. 2006, "Advantages and disadvantages of four interview techniques in qualitative research", *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, vol. 7, no. 4, pp. 1-4.
- OPSWAT 2014, *Market Share Analysis of Antivirus, Public File Sharing and Threat Detection*, OPSWAT Inc, San Francisco, United States of America, Available: <http://www2.opswat.com/about/media/reports/antivirus-market-threat-detection-january-2014>.
- Oxford Dictionaries 2014, June 10 - last update, "Standard" [Homepage of Oxford University Press], [Online]. Available: <http://www.oxforddictionaries.com/definition/english/standard> [Accessed: 2014, June 10].
- Oxford Dictionaries 2012, March 24 - last update, "Awareness" [Homepage of Oxford University Press], [Online]. Available: <http://oxforddictionaries.com/definition/awareness?q=awareness> [Accessed: 2012, March 24].
- Padayachee, K. 2012, "Taxonomy of compliant information security behavior", *Computers & Security*, vol. 31, no. 5, pp. 673-680.
- Palmer, E.J. & Devitt, P.G. 2007, "Assessment of higher order cognitive skills in undergraduate education: modified essay or multiple choice questions? Research paper", *BMC Medical Education*, vol. 7, no. 1, pp. 49-56.
- Panda Security 2011, *Panda Security Annual Report 2011 Summary*, Panda Security, Bilbao, Spain, Available: <http://press.pandasecurity.com/wp-content/uploads/2012/01/Annual-Report-PandaLabs-2011.pdf>.
- Papacharissi, Z. & Rubin, A.M. 2000, "Predictors of Internet use", *Journal of Broadcasting & Electronic Media*, vol. 44, no. 2, pp. 175-196.
- Park, C. & Lee, J.H. 2012, "Factors influencing the accessibility of online social game", *IEEE Symposium on E-Learning, E-Management and E-Services (IS3e)*, IEEE, New Jersey, United States of America, 21 - 24 October 2012, pp. 1 - 4.
- PCI Security Standards Council 2010, *PCI DSS Requirements and Security Assessment Procedures*, Payment Card Industry Data Security Standard, Wakefield, United States of America, Available: [https://www.pcisecuritystandards.org/documents/pci\\_dss\\_v2.pdf](https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf).
- Pelled, L.H., Eisenhardt, K.M. & Xin, K.R. 1999, "Exploring the black box: An analysis of work group diversity, conflict and performance", *Administrative Science Quarterly*, vol. 44, no. 1, pp. 1-28.

- Pennebaker, J.W. 2011, *The Secret Life of Pronouns: What Our Words Say About Us*, 1st edn, Bloomsbury Press, London, United Kingdom.
- Pennebaker, J.W., Chung, C.K., Ireland, M., Gonzales, A. & Booth, R.J. 2007, *The development and psychometric properties of LIWC2007*, LIWC.net, Austin, United States of America, Available: <http://www.liwc.net/LIWC2007LanguageManual.pdf>.
- Pennebaker, J.W. & King, L.A. 1999, "Linguistic styles: Language use as an individual difference", *Journal of personality and social psychology*, vol. 77, no. 6, pp. 1296-1312.
- Pennebaker, J.W., Booth, R. & Francis, M. 2007, *Linguistic inquiry and word count: LIWC [Computer software]*, 2nd edn, Pennebaker Conglomerates, Inc., Austin, United States of America.
- Pfleeger, S.L. & Kitchenham, B.A. 2001, "Principles of survey research (Part 1): Turning lemons into lemonade", *ACM SIGSOFT Software Engineering Notes*, vol. 26, no. 6, pp. 16-18.
- Plant, R. & Murrell, S. 2007, *An Executive's Guide to Information Technology: Principles, Business Models, and Terminology*, 1st edn, Cambridge University Press, Cambridge, United Kingdom.
- Polychronakis, M., Mavrommatis, P. & Provos, N. 2008, "Ghost turns zombie: exploring the life cycle of web-based malware", *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, USENIX Association, Berkeley, United States of America, 14 April 2008, pp. 11:1-11:8.
- Priebatsch, S. 2010, *The game layer on top of the world (TEDxBoston 2010)*, 1st edn, TED, Boston, United States of America.
- Protalinski, E. 2012, January 17 - last update, *Facebook to expose hackers behind Koobface worm* [Homepage of ZDNet], [Online]. Available: <http://www.zdnet.com/blog/facebook/facebook-to-expose-hackers-behind-koobface-worm/7462> [Accessed: 2012, September 19].
- Provos, N., McNamee, D., Mavrommatis, P., Wang, K. & Modadugu, N. 2007, "The ghost in the browser analysis of web-based malware", *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, USENIX Association, Berkeley, United States of America, 10 April 2007, pp. 4:1-4:9.
- R Core Team 2013, *R: A language and environment for statistical computing*, 3.0.1 edn, R Foundation for Statistical Computing, Vienna, Austria.
- Rashid, F.Y. 2012, December 05 - last update, *Sophisticated Zeus Campaign Stole €36 Million From 30,000 Bank Accounts* [Homepage of SecurityWeek], [Online]. Available: <http://www.securityweek.com/sophisticated-zeus-campaign-stole-%E2%82%AC36-million-30000-bank-accounts> [Accessed: 2012, December 18].
- Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), pp. 1-6.
- Ressler, S. 2006, "Social network analysis as an approach to combat terrorism: Past, present, and future research", *Homeland Security Affairs*, vol. 2, no. 2, pp. 1-10.
- Rezgui, Y. & Marks, A. 2008, "Information security awareness in higher education: An exploratory study", *Computers & Security*, vol. 27, no. 7-8, pp. 241-253.
- Rhee, H., Kim, C. & Ryu, Y.U. 2009, "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computers & Security*, vol. 28, no. 8, pp. 816-826.
- Rockart, J.F. & Flannery, L.S. 1983, "The management of end user computing", *Communications of the ACM*, vol. 26, no. 10, pp. 776-784.
- Rossman, R. 2010, March 13 - last update, *Federal report: Cost of Internet scams more than doubled in 2009* [Homepage of Dallas News], [Online]. Available: <http://www.dallasnews.com/business/technology/20100312-Federal-report-Cost-of-Internet-7147.ece> [Accessed: 2012, November 11].
- Rovee-Collier, C., Evancio, S. & Earley, L.A. 1995, "The time window hypothesis: Spacing effects", *Infant Behavior and Development*, vol. 18, no. 1, pp. 69-78.
- RSA, I. 2012, *The Current State of Cybercrime and What to Expect in 2012*, RSA, Massachusetts, United States of America, Available: [http://www.rsa.com/products/consumer/whitepapers/11634\\_CYBRC12\\_WP\\_0112.pdf](http://www.rsa.com/products/consumer/whitepapers/11634_CYBRC12_WP_0112.pdf).



- Russell, C. 2002, *Security Awareness – Implementing an Effective Strategy*, SANS Institute Reading Room, Swansea, United Kingdom, Available: [http://www.sans.org/reading\\_room/whitepapers/awareness/security-awareness-implementing-effective-strategy\\_418](http://www.sans.org/reading_room/whitepapers/awareness/security-awareness-implementing-effective-strategy_418).
- Ryan, R.M. & Deci, E.L. 2000, "Intrinsic and extrinsic motivations: Classic definitions and new directions", *Contemporary educational psychology*, vol. 25, no. 1, pp. 54-67.
- Ryan, T. & Xenos, S. 2011, "Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage", *Computers in Human Behavior*, vol. 27, no. 5, pp. 1658-1664.
- Sadeghian, A., Zamani, M. & Shanmugam, B. 2013, "Security Threats in Online Social Networks", *International Conference on Informatics and Creative Multimedia (ICICM)*, IEEE, New Jersey, United States of America, 4 - 6 September 2013, pp. 254-258.
- SANS 2010, *Security Awareness Roadmap*, SANS Institute, Swansea, United Kingdom, Available: <https://www.securingthehuman.org/resources/planning>.
- Saunders, M.K.K., Lewis, P. & Thornhill, A. 2012, *Research Methods for Business Students*, 6th edn, Pearson Custom Publishing, New York, United States of America.
- Saunders, M. & Tosey, P. 2012, "The Layers of Research Design", *Rapport*, vol. Winter, no. 2012/2013, pp. 58-59-59.
- Schneier, B. 1999, "Attack trees", *Dr.Dobb's journal*, vol. 24, no. 12, pp. 21-29.
- Schuba, C.L., Krsul, I.V., Kuhn, M.G., Spafford, E.H., Sundaram, A. & Zamboni, D. 1997, "Analysis of a denial of service attack on TCP", *Proceedings of the IEEE Symposium on Security and Privacy*, IEEE, New Jersey, United States, 4 - 7 May 1997, pp. 208-223.
- Secunia 2015, *Secunia Vulnerability Review 2015*, Secunia, Copenhagen, Denmark, Available: <http://secunia.com/resources/vulnerability-review/introduction/>.
- Shaw, A. 2009, *Data breach: from notification to prevention using PCI DSS*, Columbia University.
- Shaw, R.S., Chen, C.C., Harris, A.L. & Huang, H. 2009, "The impact of information richness on information security awareness training effectiveness", *Computers & Education*, vol. 52, no. 1, pp. 92-100.
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania, USA. pp. 88-99.
- Shin, D.H. & Shin, Y.J. 2011, "Why do people play social network games?", *Computers in Human Behavior*, vol. 27, no. 2, pp. 852-861.
- Sieber, T. 2013, April 18 - last update, *Facebook Friend Requests: Unwritten Rules & Hidden Settings* [Homepage of MakeUseOf], [Online]. Available: <http://www.makeuseof.com/tag/facebook-friend-requests-unwritten-rules-hidden-settings-weekly-facebook-tips/> [Accessed: 2014, January 22].
- Sood, A.K., Bansal, R. & Enbody, R.J. 2013, "Cybercrime: Dissecting the State of Underground Enterprise", *Internet Computing, IEEE*, vol. 17, no. 1, pp. 60-68.
- Sophos 2014, *Security Threat Report 2014*, Sophos, Abingdon, United Kingdom, Available: <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf>.
- Sophos 2013, *Security Threat Report 2013*, Sophos, Abingdon, United Kingdom, Available: <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf>.
- Stallman, R. 1991, *Gnu general public license*, 1st edn, Free Software Foundation, Massachusetts, United States of America.
- Stanford, D. & Robertson, J. 2014, September 2 - last update, *Apple Probes Report iCloud Was Hacked to Gain Stars' Nude Photos* [Homepage of Bloomberg L.P], [Online]. Available: <http://www.bloomberg.com/news/2014-09-01/apple-probes-if-hacker-got-stars-nude-photos-from-icloud.html> [Accessed: 2014, November 11].
- Stanton, J.M., Stam, K.R., Mastrangelo, P. & Jolton, J. 2005, "Analysis of end user security behaviors", *Computers & Security*, vol. 24, no. 2, pp. 124-133.

Stewart, G. & Austen, J. 2009, *Maximising the Effectiveness of Information Security Awareness*, Royal Holloway University of London, London, Available: [http://media.techtarget.com/searchSecurityUK/downloads/RHUL\\_Stewart\\_FINALFINAL.pdf](http://media.techtarget.com/searchSecurityUK/downloads/RHUL_Stewart_FINALFINAL.pdf).

Stewart, J. 2006, "Behavioural malware analysis using Sandnets", *Computer Fraud & Security*, vol. 2006, no. 12, pp. 4-6.

Stone-Gross, B., Holz, T., Stringhini, G. & Vigna, G. 2011, "The underground economy of spam: A botmaster's perspective of coordinating large-scale spam campaigns", *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, USENIX Association, Boston, United States of America, 29 March 2011, pp. 4-12.

Subrahmanyam, K., Reich, S.M., Waechter, N. & Espinoza, G. 2008, "Online and offline social networks: Use of social networking sites by emerging adults", *Journal of Applied Developmental Psychology*, vol. 29, no. 6, pp. 420-433.

Swart, W. & Afrika, M. 2012, January 15 - last update, *It was a happy New Year's Day for gang who pulled off...R42m Postbank heist* [Homepage of Time Live], [Online]. Available: <http://www.timeslive.co.za/local/2012/01/15/it-was-a-happy-new-year-s-day-for-gang-who-pulled-off...r42m-postbank-heist> [Accessed: 2012, April 13].

Szewczyk, P. & Furnell, S. 2009, "Assessing the online security awareness of Australian Internet users", *Proceedings of 8th Annual Security Conference*, Information Institute Publishing, Washington, United States of America, 15 -16 April 2009, pp. 58:1-58:9.

Theobald, W. & Dunsmore, H.E. 2000, "Chapter 5 - Web browsers" in *Internet Resources for Leisure and Tourism*, 1st edn, Butterworth-Heinemann, Oxford, United Kingdom, pp. 72-88.

Thomas, K. & Nicol, D.M. 2010, "The Koobface botnet and the rise of social malware", *5th International Conference on Malicious and Unwanted Software (MALWARE)*, IEEE, New Jersey, United States, 19 - 20 October 2010, pp. 63-70.

Thomson, M.E. & von Solms, R. 1998, "Information security awareness: educating your users effectively", *Information management & computer security*, vol. 6, no. 4, pp. 167-173.

Timm, C. 2010, "Evil Twin Attacks" in *Seven Deadliest Social Network Attacks* Syngress, Boston, pp. 63-82.

Tomsho, G. 2011, *Guide to networking essentials*, Cengage Learning, Boston.

UK Essays 2013, November 12 - last update, *Explanation Of The Concept Of Research Onion Psychology Essay* [Homepage of UK Essays], [Online]. Available: <http://www.ukessays.com/essays/psychology/explanation-of-the-concept-of-research-onion-psychology-essay.php> [Accessed: 2015, July 04].

University of South Africa 2007, *UNISA: Policy on Research Ethics*, UNISA Available: [http://www.unisa.ac.za/contents/colleges/col\\_grad\\_studies/docs/Policy\\_research\\_ethics\\_21September2007.pdf](http://www.unisa.ac.za/contents/colleges/col_grad_studies/docs/Policy_research_ethics_21September2007.pdf).

University of Venda 2013, September 12 - last update, *Degree Programme in Computer Science and Information Systems* [Homepage of UNIVEN], [Online]. Available: <http://www.univen.ac.za/index.php?Entity=Computer%20Science%20and%20Info%20Sciences&Sch=8> [Accessed: 2013, September 12].

US Government Organization 1996, *Health Insurance Portability and Accountability Act*, U.S. Government Printing Office Available: <http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf>.

Veerasamy, N. & Grobler, M. 2011, "Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure", *The Proceedings of the 6th International Conference on Information Warfare and Security*, ed. J. Ryan, Academic Conferences Limited, Reading, United Kingdom, 17 - 18 March 2011, pp. 172-187.

Vergano, D. 2011, February 27 - last update, *Terrorists taunts may tell attack timing* [Homepage of USA Today], [Online]. Available: [http://www.usatoday.com/tech/science/columnist/vergano/2011-02-27-terrorist-words\\_N.htm](http://www.usatoday.com/tech/science/columnist/vergano/2011-02-27-terrorist-words_N.htm) [Accessed: 2012, January 23].

Vollrath, M. & Torgersen, S. 2000, "Personality types and coping", *Personality and Individual Differences*, vol. 29, no. 2, pp. 367-378.

- Wang, C., Zhang, D., Lu, H., Zhao, J., Zhang, Z. & Zheng, Z. 2014, "An experimental study on firewall performance: Dive into the bottleneck for firewall effectiveness", *10th International Conference on Information Assurance and Security (IAS)*, IEEE, New Jersey, United States of America, 28 - 30 November 2014, pp. 71-76.
- Webb, J., Ahmad, A., Maynard, S.B. & Shanks, G. 2014, "A situation awareness model for information security risk management", *Computers & Security*, vol. 44, pp. 1-15.
- Whitlock, C. 2011, October 10 - last update, *New survey data from Experian's ProtectMyID™ reveals people are making it easy for cybercriminals to steal their identity* [Homepage of StrategyOne Research], [Online]. Available: <http://press.experian.com/United-States/Press-Release/people-are-making-it-easy-for-cybercriminals-to-steal-their-identity.aspx?&p=1> [Accessed: 2012, January 30].
- Wikia 2015, April 29 - last update, *Malicious payload* [Homepage of Wikia], [Online]. Available: [http://itlaw.wikia.com/wiki/Malicious\\_payload](http://itlaw.wikia.com/wiki/Malicious_payload) [Accessed: 2015, April 29].
- Wilshusen, G.C. & Lawrence, A. 2011, *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements*, United States Government Accountability Office, Washington, United States of America, Available: <http://www.gao.gov/products/GAO-12-137>.
- Wilson, M. & Hash, J. 2003, *Building an information technology security awareness and training program (NIST SP 800-50)*, National Institute of Standards and Technology (NIST), Washington, United States of America, Available: <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>.
- Woodford, K. & Bancroft, P. 2006, "Using multiple choice questions effectively in information technology education", *Proceedings of the 8th Australasian Conference on Computing Education*, Australian Computer Society, Inc., Darlinghurst, Australia, 16 - 19 January 2006, pp. 948-955.
- Yohannis, A.R., Prabowo, Y.D. & Waworuntu, A. 2014, "Defining gamification: From lexical meaning and process viewpoint towards a gameful reality", *International Conference on Information Technology Systems and Innovation (ICITSI)*, IEEE, New Jersey, United States of America, 24 - 27 November 2014, pp. 284-289.
- Zhang, L., Choffnes, D., Levin, D., Dumitras, T., Mislove, A., Schulman, A. & Wilson, C. 2014, "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed", *IMC '14: Proceedings of the 2014 Conference on Internet Measurement Conference*, ACM, New York, United States of America, 05 - 07 November 2014, pp. 489-502.
- Zhu, D. & Chin, E. 2007, *Detection of VM-Aware Malware*, University of Berkeley, Berkeley, United Kingdom, Available: [http://radlab.cs.berkeley.edu/w/upload/3/3d/Detecting\\_VM\\_Aware\\_Malware.pdf](http://radlab.cs.berkeley.edu/w/upload/3/3d/Detecting_VM_Aware_Malware.pdf).
- Zorz, Z. 2014a, October 23 - last update, *Attackers bypass Sandworm patch with new 0-day* [Homepage of Net-Security], [Online]. Available: <http://www.net-security.org/secworld.php?id=17524> [Accessed: 2014, October 25].
- Zorz, Z. 2014b, October 15 - last update, *POODLE vulnerability: The end of life of SSL 3.0* [Homepage of Net-Security], [Online]. Available: <http://www.net-security.org/secworld.php?id=17495> [Accessed: 2014, October 28].
- Zyda, M., Mayberry, A., Wardynski, C., Shilling, R. & Davis, M. 2003, "The MOVES institute's America's army operations game", *Proceedings of the 2003 symposium on Interactive 3D graphics*, ACM, New York, United States of America, 27 - 30 April 2003, pp. 219-220.

## Appendix A Ethical Clearance Certificate

 	
Mr A Labuschagne (47298022) School of Computing UNISA Pretoria	23 August 2012
<b>TO WHOM IT MAY CONCERN</b>	
<b>Permission to conduct MTech research project</b>	<b>Ref: 033/AL/2012</b>
The request for ethical approval for your MTech research project entitled: "Evaluating the effectiveness of a social networking site game to conduct a security awareness program to non-Information Technology (IT) students within South Africa." refers.	
The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.	
Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.	
We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL: <a href="http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf">http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf</a>	
Yours sincerely	
	
<b>Prof HH Lotriet</b> Chair: School of Computing Ethics Sub-Committee	
	University of South Africa College of Science, Engineering and Technology Preller Street, Muckleneuk Ridge, City of Tshwane PO Box 392 UNISA 0003 South Africa Telephone + 27 12 429 6122 Facsimile + 27 12 429 6848 <a href="http://www.unisa.ac.za/cset">www.unisa.ac.za/cset</a>

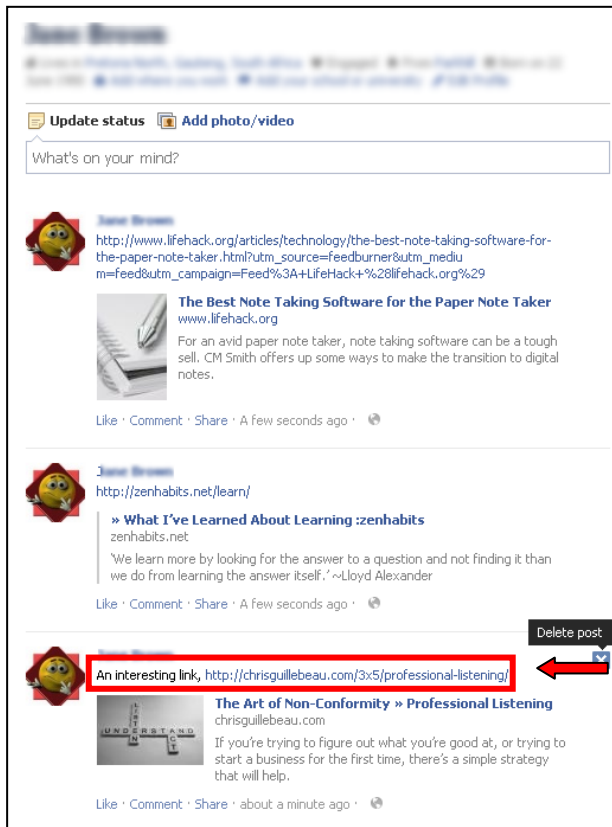


## Appendix B Questionnaire (Pre Assessment)

- 1) Should you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter or your personal email accounts?
  - Yes
  - **No**
- 2) Should you provide others (for example your co-worker, friend or system administrator) with your passwords?
  - Yes
  - **No**
- 3) Select the strongest password from the list
  - Aassbb
  - Qwerty
  - 1234
  - **!@#QAZ2012**
- 4) Select the weakest password from the list
  - plmqwe20@!
  - !@#mnia#@!
  - **aabbcc**
  - \*#!QAQ12
- 5) What does the term "Brute Force" mean?
  - Hacking into a system
  - Cracking a password
  - **Cracking a password using all possible combinations**
  - None of the above
- 6) Which of the following is not classified as malware?
  - Virus
  - Trojan Horse
  - Worm
  - **Social Engineering**

- 7) Which of the following is classified as malware?
- CyberBully
  - SPAM
  - Denial of Service
  - **Worm**
  - Your computer (not just your connection speed) slows down significantly whether online or offline
- 8) What is a/are the sign(s) that your computer might be infected with malware?
- Strange problems occur within windows, (performance issues, programs not working as they should, etc)
  - Your computer (not just your connection speed) slows down significantly whether online or offline
  - **All of the above**
- 9) What does the term "Malware" mean?
- It is any software package which automatically renders advertisements
  - **It is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer system**
  - Software that protects your system from infections
  - None of the above
- 10) You installed an Anti-Virus (AV) software application on your personal computer. Is your computer safe from malware infections?
- Yes
  - **No**
- 11) You see the following message on your wall (timeline). The Wall (timeline) is a place to post and share content with your friends.

A study regarding the effectiveness of game play as part of an information security awareness program for novices



Is it safe to click on the link, to another web page, indicated in the image?

- Yes
- No

12) You see the following message on your wall (timeline). The Wall (timeline) is a place to post and share content with your friends.

A study regarding the effectiveness of game play as part of an information security awareness program for novices



Is it safe to click on the link, to another web page, indicated in the image?

- Yes
- **No**

13) You receive the following message: "About your job application..." What type of attack can this be?

- Cyber Bully
- **Social Engineering**
- Denial of Service
- Spam

14) Select the most likely reason from the list, why this could be a fake Facebook profile?



- It is a real Facebook profile
- **The activity on the wall**
- Number of friends
- The birthday displayed of the profile

15) On Facebook, do you have controls which allows you to share only specific information, for example your list of friends?

- **Yes**
- No

16) Can your computer get infected with malware by visiting a website?

- No
- **Yes**

17) Should you update your web browser regularly?

- No
- **Yes**

18) Which of the following step(s) can be used to protect your web browser against attacks?

- Keep your browser(s) updated and patched, and set to auto update
- Keep your operating system updated and patched
- Use anti-virus and anti-spyware software and keep them updated
- **All of the above**

19) Which factor(s) contribute to increasing the threat from software attacks that take advantage of vulnerable web browsers?

- Web page addresses can be disguised or take you to an unexpected site
- Many web browsers are configured to provide increased functionality at the cost of decreased security
- New security vulnerabilities may have been discovered since the software was configured and packaged by the manufacturer
- **All of the above**

20) If you have updated your web browser to the latest version, can you still be infected with malware?

- No
- **Yes**


21) What does the term "Phishing" mean?

- Catching fish in the sea or a dam
- An incident in which a user or organization is deprived of the services of a resource they would normally expect to have
- **A form of attack that typically includes email and fraudulent Websites resembling legitimate ones**
- None of the above

22) Phishing is a way of attempting to acquire information. What type of information?

- Usernames
- Passwords
- credit card
- **All of the above**

23) What type of attack is shown in the image?



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.  
To resolve this problem please visit link below and re-enter your account information:

[https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co\\_partnerId=2&siteid=0](https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0)

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.


Regards,  
Safeharbor Department eBay, Inc  
The eBay team  
This is an automatic message, please do not reply

- **Phishing**
- Denial of Service
- Malware
- CyberBully

24) What type of attack is shown in the image?

**From:** Visa Service Department <activate@verified.visa.com>  
**Subject:** **Activate Now for Verified by Visa**  
**Date:** November 30, 2005 10:30:49 AM PST  
**To:** Vaughn Aubuchon

---



---

Dear Visa® customer,

**Before activating your card, read this important information for cardholders!**

You have been sent this invitation because the records of Visa Corporate indicate you are a current or former Visa card holder. To ensure your Visa card's security, it is important that you protect your Visa card online with a personal password. Please take a moment, and activate for Verified by Visa now.

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

[Activate Now for Verified by Visa](#)

Thank you for your support.  
Visa Service Department

- **Phishing**
- Denial of Service
- Malware
- CyberBully

25) Which of the following is not a phishing technique?

- Phishing
- Spear Phishing
- Whaling
- **None of the above**



26) What does the term "CyberBully" mean?

- **The use of the Internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner**
- The art of manipulating people into performing actions or divulging confidential information
- An incident in which a user or organization is deprived of the services of a resource they would normally expect to have
- None of the above

27) What type of attack is shown in the image?



- Denial of Service
- Malware
- **CyberBully**
- Social Engineering

28) Which of the following is a/are method(s) used to cyber bully others?

- Email
- Short Message Service (SMS)
- Chat rooms
- **All of the above**

29) Which of the following is a/are example(s) of direct cyber bully attacks?

- Instant Messaging/Text Messaging Harassment
- Stealing Passwords
- Blogs

- **All of the above**

30) What is a/are some warning sign(s) that indicate a child is being cyber bullied?

- Is happy all the time
- **Appears to be angry, depressed or frustrated after using the computer or other electronic devices**
- Spend time on the computer
- All of the above

31) What does the term "Spam" mean?

- **Flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it**
- Food which can be bought for dogs
- A form of deception
- None of the above

32) What type of attack is shown in the image?

```
PROJECT MANAGER
NIGERIA NATIONAL PETROLEUM CORPORATION
FOLOMO -COMPLEX LAGOS NIGERIA
ATTN SIR/ MADAM

I am the project manager withthe Nigeria National petroleum Corporation (NNPC).
I know you will besurprise to receive this kind of letter seeking for
yourassistance.

To be cadid, I got your e-mail address through aclose relation of mine who is
now with the Nigeria Chamber of commerce(NCC)though I did not disclosed to him
what I will use it for as I onlyrequested for one.

Now the business in question is the transfer ofUS$25.5m .
This sum came as an over invoiced sum which wedid purposely, during when my
corporation awarded contract to someforeign firms which I as the project manager
masterminded the wholecontract, which the foreign contractors was dully received
their totalcontract amount leaving this over invoiced sum of USD$25.5m floating
inthe union bank Nigerian PLC, to be transferred to a foreign bankaccount. We
the official concern are still active service, and theCivil rule of conduct does
not warrant us top operate offshore account.That is the reason why we are
strongly seeking for your assistancein proving your bank information's where we
can transfer this fund.Please, you are very important in this transaction as
every documentscovering the transfer of this fund will be in your name.

So all whatwe are in need now is your banking information and ability to keep
ittop secret based on the nature of it all. We have mapped out 30% ofUS$25.5m to
be for you the account owner, 60% for us while 10% ismapped out for any process
of expenses to be incurred on the process ofthis transfer whether locally here
or Abroad. On receipt of your bankinformation's within 14 working days. This
fund will be in yournominated account.

I will be very grateful to receive thisinformation from you, and also pleased
that you should not betray thetrust I imposed in you.
```

- **Scam**
- Malware
- Phishing

- None of the above

33) What type of attack is shown in the image?



- **Scam**
- Malware
- Phishing
- None of the above

34) Scams can contain the following:

- Alarmist messages and threats of account closures
- Promises of money for little or no effort
- Deals that sound too good to be true
- **All of the above**

35) Which of the following is a/are scam prevention tip(s)?

- Take care when clicking on links in an email.
- Do not respond to emails, phone calls, text messages, or instant messages that ask for private information
- Before entering any personal information, make sure the website is secure
- **All of the above**

## Appendix C Questionnaire (Post Assessment 1)

- 1) Should you log into work accounts using public computers, such as from a library, cyber café or hotel lobby?

- Yes
  - **No**
- 2) The system administrator from your company calls you and asks you for your password. Should you provide him with your password?
- **No**
  - Yes
- 3) Select the strongest password from the list
- Zxcvb
  - 123456
  - !@#\$%
  - **#@!2012qPLO#@!**
- 4) Select the weakest password from the list
- **123456**
  - qazWSXedc!@#
  - aa2012bb2009#@!
  - 3?4<5>6!
- 5) The following is not a way of obtaining a password:
- Keyloggers
  - Sniffers
  - Web browser exploitation of cookies
  - **Sandboxing**
- 6) Which of the following is not classified as malware?
- Worm
  - **Denial of Service**
  - Trojan Horse
  - Virus
- 7) Which of the following is classified as malware?
- CyberBully
  - SPAM
  - Denial of Service
  - **Trojan Horse**
- 8) What is a/are the sign(s) that your computer might be infected with malware?

- Your firewall and antivirus programs are frequently turned off automatically
- Your network connection's activity lights blink a lot, when you are not actively doing anything on the internet
- You are unable to stop the excessive popup windows that appears from nowhere
- **All of the above**

9) What does the term "Spyware" mean?

- **Any technology that aids in gathering information about a person or organization without their knowledge**
- Software that protects your system from infections.
- Any software designed to cause damage to a single computer, server, or computer network
- None of the above

10) You have downloaded software from a link in an email that was sent to you by someone you do not know. Should you install the software?

- Yes
- **No**

11) You see the following message on your wall (timeline). The Wall (timeline) is a place to post and share content with your friends.

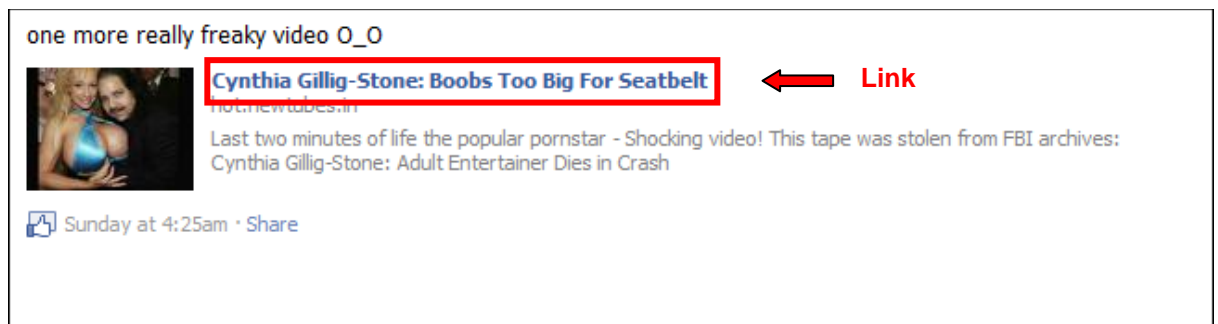
A study regarding the effectiveness of game play as part of an information security awareness program for novices



Is it safe to click on the link, to another web page, indicated in the image?

- Yes
- No

12) You see the following message on your wall (timeline). The Wall (timeline) is a place to post and share content with your friends.



Is it safe to click on the link, to another web page, indicated in the image?

- Yes
- No

13) You receive the following message: "@Twitterguy, what do you think about what Obama said on #cybersecurity? http://shar.es/HNGAt." What type of attack can this be?

- Cyber Bully
- **Social Engineering**
- Denial of Service
- Spam

14) Select the most likely reason from the list, why this could be a fake Facebook profile?



- The profile picture does not depict a real person
- The number of friends
- The user only uploaded one picture into the photos section
- **All of the above**

15) Should you provide personal information, such as your physical address, on Facebook?

- Yes
- **No**

16) Can your computer get infected with malware by reading a portable document format (PDF) file?

- **Yes**
- No

17) You open your web browser and a message appears that you need to update your web browser. What should you do next?

- Close the message
- Continue to your favourite website
- **Update the web browser**
- None of the above

18) Which of the following step(s) can be used to protect against web browser attacks?

- Install a firewall and keep it updated and patched
- Keep your applications (programs) updated and patched, particularly if they work with your browser (such as multi-media programs and plug-ins used to enable running of videos, for example)
- **All of the above**
- None of the above

19) Which factor(s) contribute to increasing the threat from software attacks that take advantage of vulnerable web browsers

- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.
- Third-party software may not have a mechanism for receiving security updates
- Many websites require that users enable certain features or install more software, putting the computer at additional risk.
- **All of the above**

20) Does 3rd party software for example Flash, Acrobat Reader or Windows Media Player create a potential security risk?

- **Yes**



- No

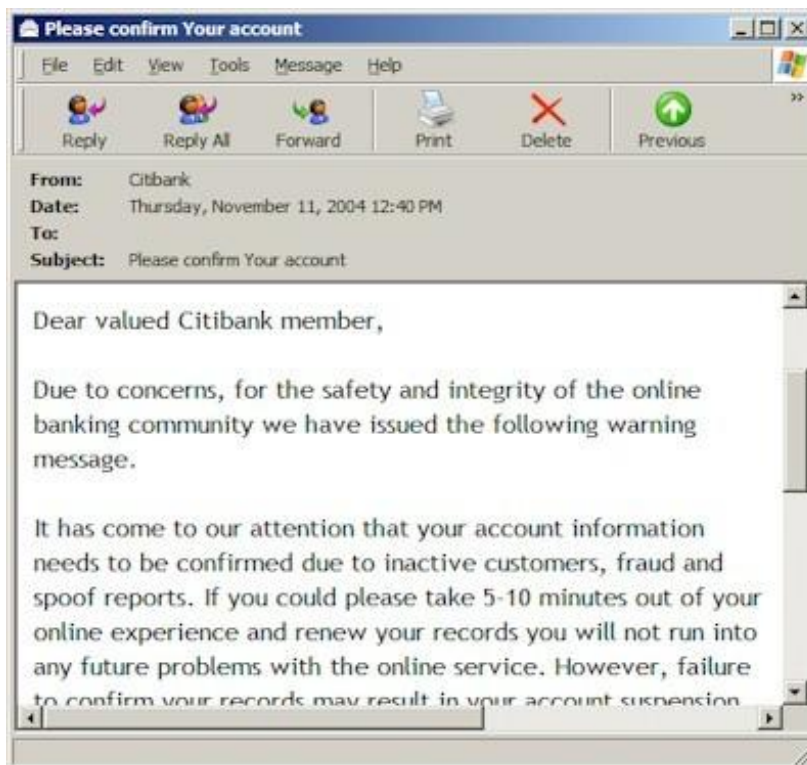
21) Phishing email messages, websites, and phone calls are designed to

- Infect your computer
- **Steal your money/personal information such as passwords and account numbers**
- Provide free access to Internet
- None of the above

22) Which of the following information listed, is the most useful to phishing attacks?

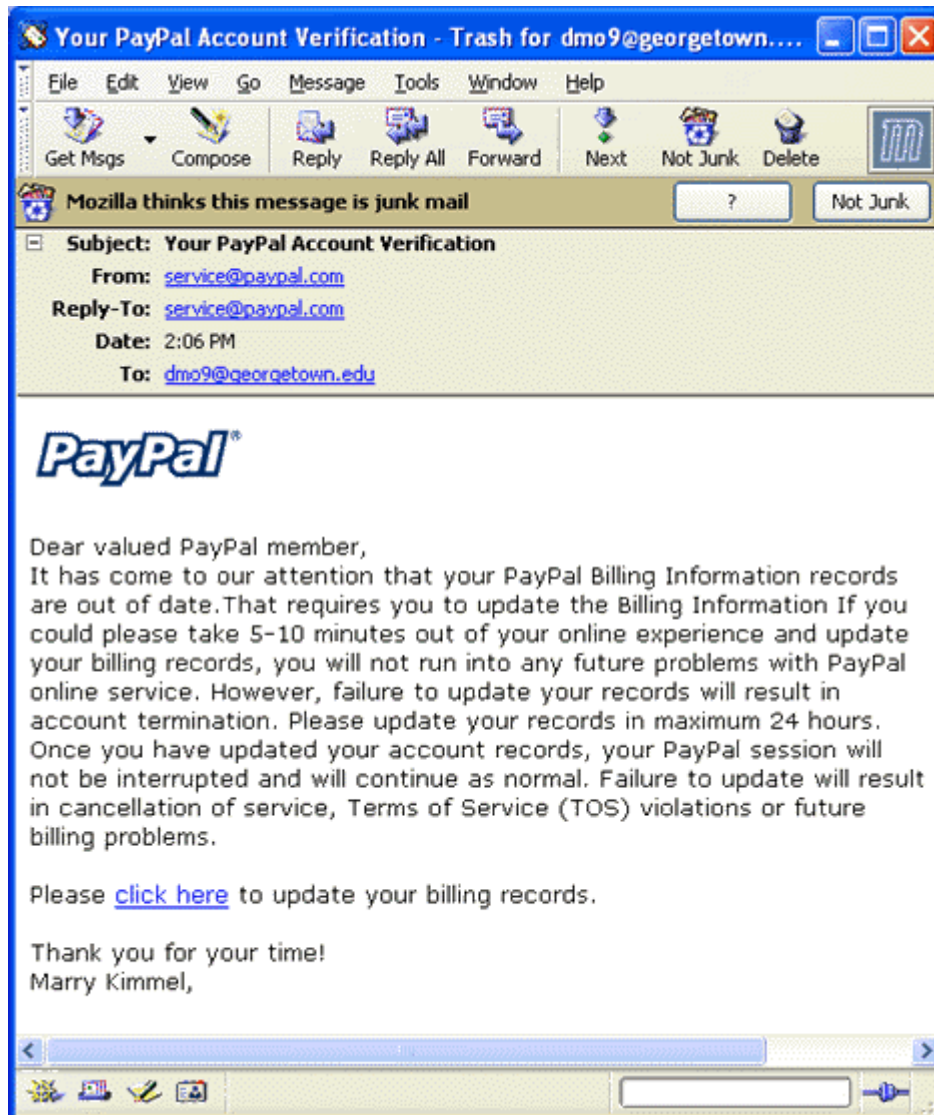
- Gender
- **Credit card number**
- Interests
- All of the above

23) What type of attack is shown in the image?



- **Phishing**
- Denial of Service Attack
- Malware
- CyberBully

24) What type of attack is shown in the image?



- **Phishing**
- Denial of Service Attack
- Malware
- CyberBully

25) Which of the following is a/are phishing technique(s)?

- Clone Phishing
- Spear Phishing
- Whaling
- **All of the above**

26) Being a victim of cyberbullying can be a common and painful experience. Some youths who cyberbully

- Pretend they are other people online to trick others
- Spread lies and rumours about victims
- Trick people into revealing personal information
- **All of the above**

27) What type of attack is shown in the image?



- Denial of Service
- Malware
- **CyberBully**
- Social Engineering

28) Which of the following is a/are method(s) used to cyberbully others?

- A bash board
- Websites
- Mobile phones
- **All of the above**

29) Which of the following is a/are example(s) of Cyberbullying by proxy?

- Websites
- Sending pictures through email and Cell phone
- Internet polling
- **None of the above**

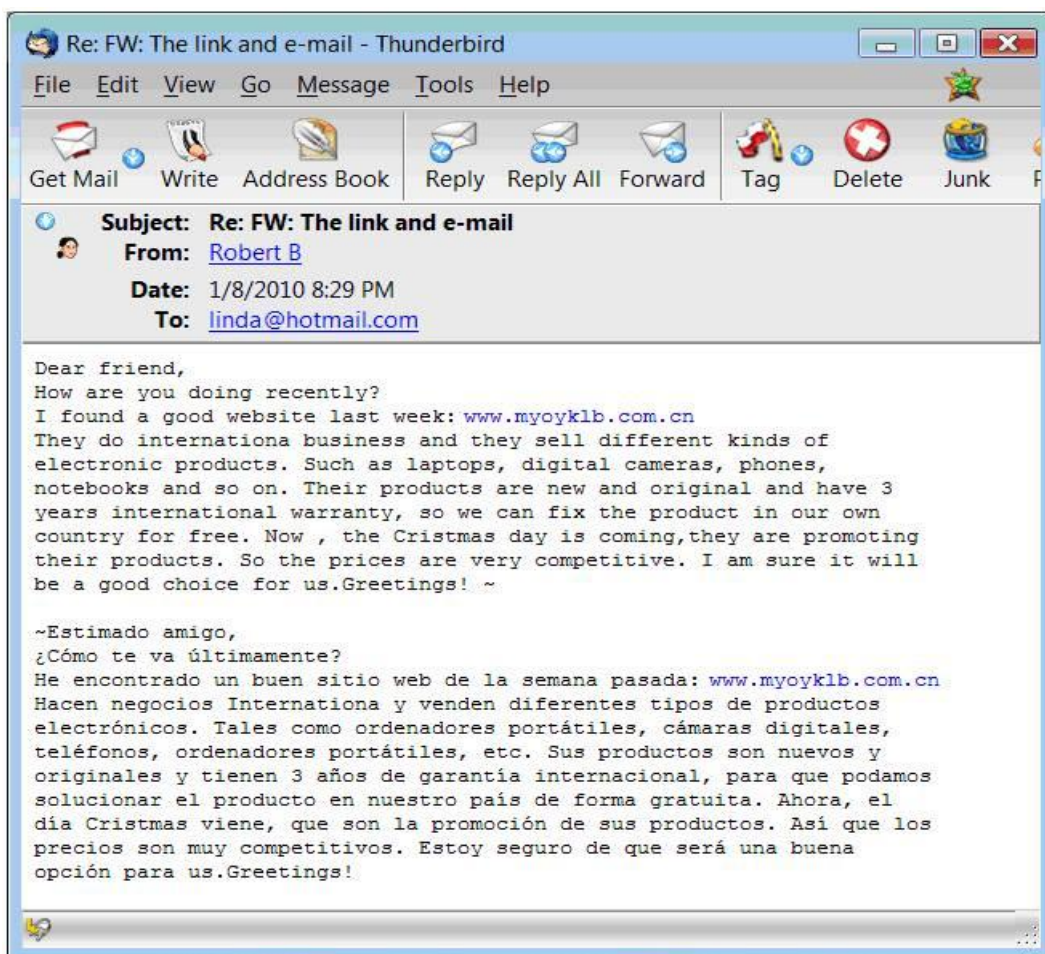
30) What is a/are some warning sign(s) that indicate a child is being cyber bullied?

- Appears to be happy
- Loves going to school and communicating by using electronic devices to keep in touch with friends
- **Either unexpectedly stops using the computer or other electronic devices or displays an acute increase in use**
- All of the above

31)What to do if you think you have been a victim of a scam

- Change the passwords or personal identification number (PIN)s on all your online accounts that you think might be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent email message.
- **All of the above**

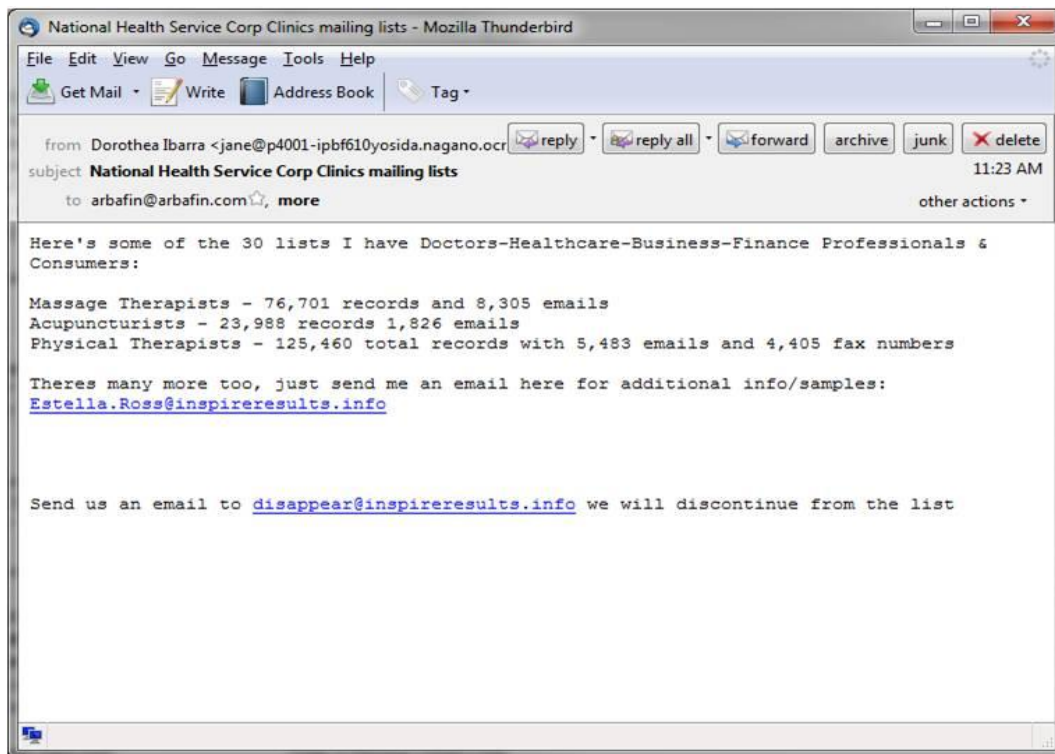
32)What type of attack is shown in the image?



- Malware
- **Scam**
- Phishing
- None of the above

33)What type of attack is shown in the image?

A study regarding the effectiveness of game play as part of an information security awareness program for novices



- Malware
- **Scam**
- Phishing
- None of the above

34) Scams can contain the following:

- Requests to donate to a charitable organization after a disaster that has been in the news
- Deals that sound too good to be true
- Alarmist messages and threats of account closures
- **All of the above**

35) Which of the following is a/are scam prevention tip(s)?

- If an email asks you to "verify your account" then you should immediately ignore this altogether
- If you should receive any kind of email which states "if you do not respond within 48 hours then your account will be suspended or closed" ignore it
- Look up the proper phone number or website URL on the paperwork you receive from the company
- **All of the above**

## Appendix D Questionnaire (Post Assessment 2)

- 1) Should you log out of your email, Facebook or Twitter accounts before you leave your computer?
  - **Yes**
  - No
- 2) Your bank contacts you and informs you that your automated teller machine (ATM) card has a problem. The bank requests your pin number to fix the problem. Do you provide them with your password?
  - Yes
  - **No**
- 3) Select the strongest password from the list
  - **#\$%CTveQA@**
  - 11223344
  - Qwaszx
  - Admin
- 4) Select the weakest password from the list
  - mnia1212
  - **admin**
  - !@##@!45
  - 12!@21!@21!@>
- 5) What does term "Bracketing" mean within password management?
  - No meaning
  - **Wrap password in one or more symbols (for example james becomes <james>)**
  - Removing characters (for example james becomes ame)
  - None of the above
- 6) Which of the following is not classified as malware?
  - Denial of Service
  - SPAM
  - CyberBully
  - **None of the above**

7) Which of the following is classified as malware?

- CyberBully
- SPAM
- Denial of Service
- **All of the above**

8) What is a/are the sign(s) that your computer might be infected with malware?

- You get frequent alerts from your firewall about an unknown program or process trying to access the internet
- Strange problems occur within windows, (performance issues, programs not working as they should, etc)
- You get a lot of bounced back mail and see evidence of emails being sent without your knowledge
- **All of the above**

9) What does the term "Ransomware" mean?

- Software that protects your system from infections.
- Any software designed to cause damage to a single computer, server, or computer network
- **Software restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed**
- None of the above

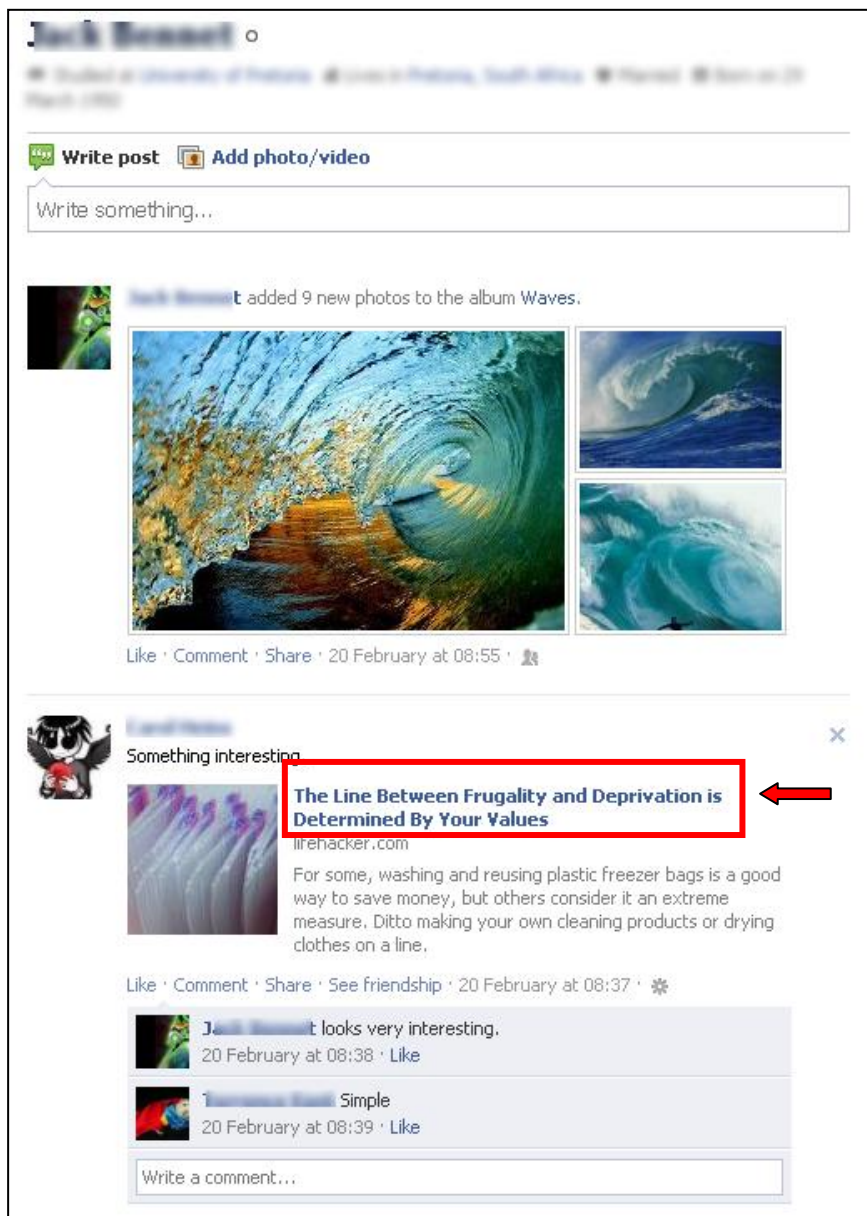
10) Is Anti-virus (AV) software automatically installed on your computer?

- Yes
- **No**

11) You see the following message on your wall (timeline). The Wall (timeline) is a place to post and share content with your friends.



A study regarding the effectiveness of game play as part of an information security awareness program for novices

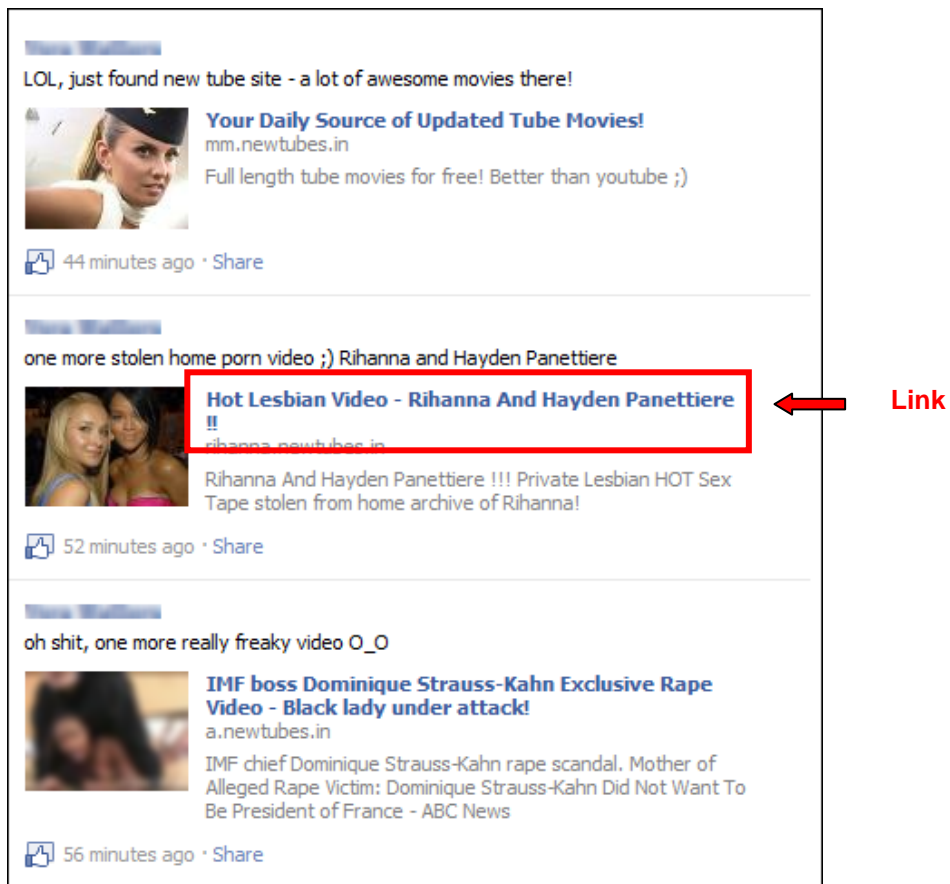


Is it safe to click on the link, to another web page, indicated in the image?

- Yes
- No

12) You see the following message on your wall (timeline). The Wall (timeline) is a place to post and share content with your friends.





Is it safe to click on the link, to another web page, indicated in the image?

- Yes
- **No**

13) You receive the following message: *"Donate to the hurricane recovery efforts!"*

What type of attack can this be?

- CyberBully
- **Social Engineering**
- Denial of Service
- Spam

14) Select the most likely reason from the list, why this could be a fake Facebook profile?

A study regarding the effectiveness of game play as part of an information security awareness program for novices



- Profile image
- Number of friends
- Activity on wall
- **All of the above**

15) On Facebook, you receive a "Friend request" from someone you do not know. What should you do?

- Accept request
- **Send message to the person to request more information**
- Get contact number from the person's Facebook profile and give him/she a call
- None of the above

16) Can your computer get infected with malware by visiting a viewing a Flash movie?

- No
- **Yes**

17) Should you enable the auto update feature within the web browser? This feature notifies the user when new updates are available to the user.

- **Yes, enable the auto update feature**
- No, do not enable auto update
- There is no need, the web browser is always safe to use
- None of the above

18) Which of the following steps can be used to protect against web browser attacks?

- Block pop-up windows, as this may help prevent malicious software from being downloaded to your computer
- Consider disabling JavaScript, Java, and ActiveX controls when not being used. Activate these features when necessary
- Keep your browser(s) updated and patched, and set to auto update
- **All of the above**

19) Which factor(s) contribute to increasing the threat from software attacks that take advantage of vulnerable web browsers

- Many websites require that users enable certain features or install more software, putting the computer at additional risk
- Many users do not know how to configure their web browsers securely
- Many users are unwilling to enable or disable functionality as required to secure their web browser
- **All of the above**

20) Which of the following is a/are specific web browser feature(s) that presents a risk?

- ActiveX
- Plug-ins
- Cookies
- JavaScript
- **All of the above**

21) What does a phishing attack in an email message consist of

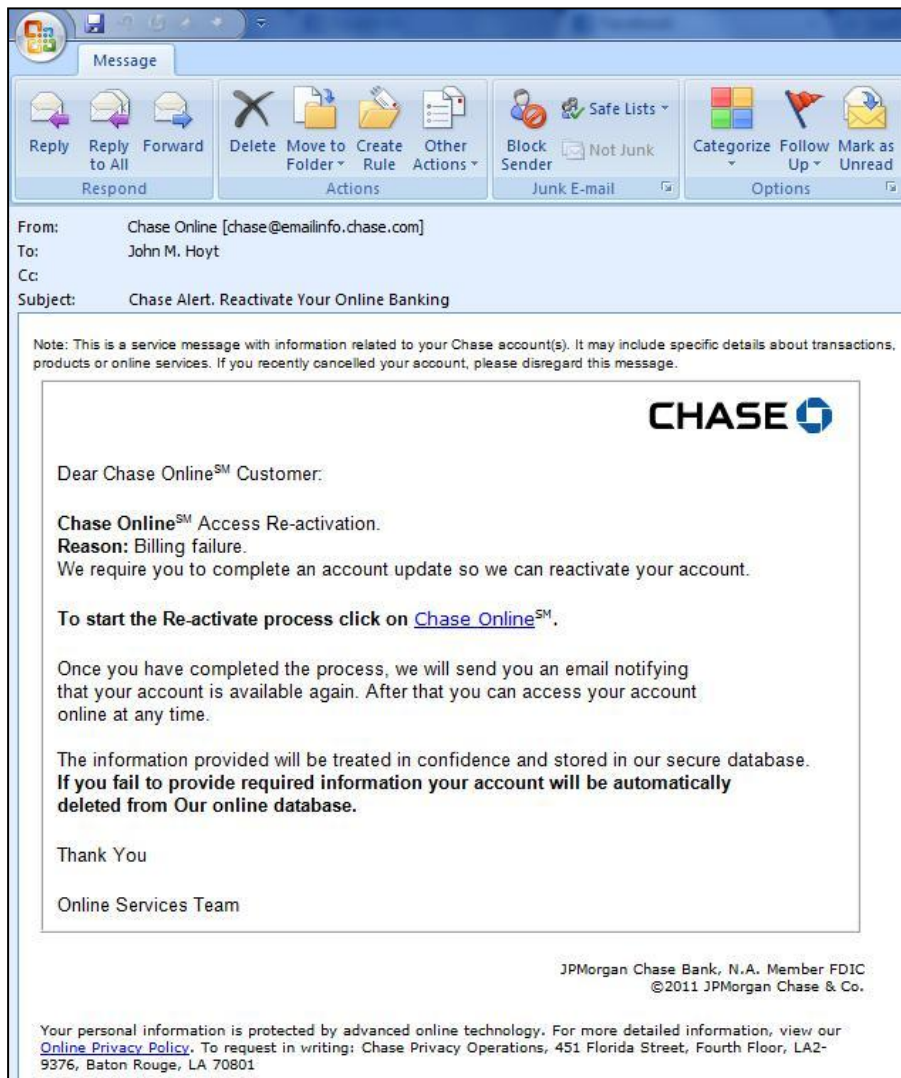
- Spelling and bad grammar
- Unknown web links within the email

- A threatening message within the email, for example your account has been hacked
- **All of the above**

22) Which of the following information is the least useful to phishing attacks?

- Physical Address
- Username
- Password
- **Gender**

23) What type of attack is shown in the image?



- **Phishing**
- Denial of Service
- Malware

- CyberBully

24)What type of attack is shown in the image?



- **Phishing**
- Denial of Service
- Malware
- CyberBully

25)Which of the following is not a phishing technique?

- Spear Phishing
- Clone Phishing
- Whaling
- **Sharking**

26)Being a victim of cyberbullying can be a common and painful experience. Some youths who cyberbully

- Send or forward mean text messages
- Post pictures of victims without their consent
- Pretend they are other people online to trick others
- **All of the above**

27) What type of attack is shown in the image?



- Denial of Service
- Malware
- **CyberBully**
- Social Engineering

28) Which of the following are method(s) used to cyberbully others?

- SMSs
- Chatrooms
- Websites
- **All of the above**

29) Which of the following is a/are example(s) of direct cyber bully attacks?

- Interactive Gaming
- Sending Malicious code
- Sending porn and other junk email and instant messaging (IM)
- **All of the above**

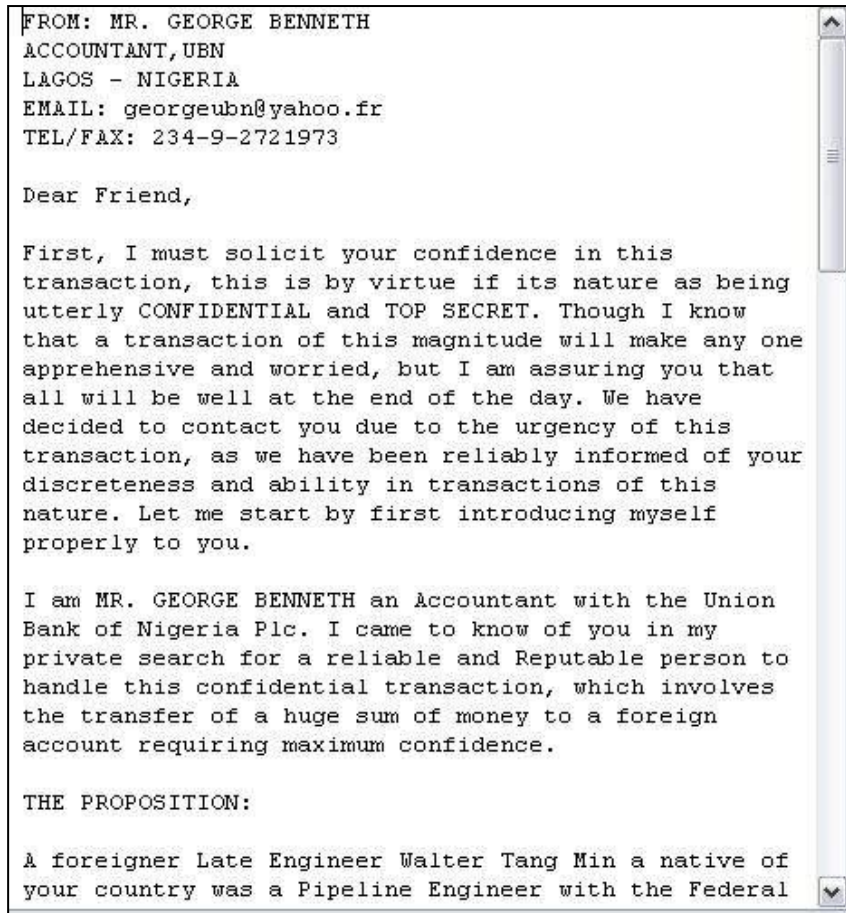
30) What is a/are some warning sign(s) that indicate a child is being cyber bullied?

- Becomes abnormally withdrawn from usual friends and family members
- Avoids discussions about what he or she is doing on the computer or other electronic devices.
- Appears to be angry, depressed or frustrated after using the computer or other electronic devices
- **All of the above**

31) Should you open email attachments from people that you do not know

- Yes
- **No**

32) What type of attack is shown in the image?



- Phishing
- Malware
- **Scam**
- None of the above

33) What type of attack is shown in the image?



Greetings to you my friend,

I know this will come to you as a surprise because you do not know me.  
I am John Alison I work in Central Bank of Nigeria, packaging and courier department.

I got your contact among others from a search on the internet and I was inspired to seek your  
co-operation, I want you to help me clear this consignment that is already in the Europe which I shipped  
through our CBN accredited courier agent. The content of the package is \$20,000,000.00 all in \$100 bills,  
but the courier company does not know that the consignment contains money.

All I want you to do for me now is to give me your mailing address, your private phone and fax number,  
and I believe that at the end of the day you will have 50% and 50% will be for me. My identity must not  
be revealed to anybody.

If this arrangement is okay by you, you can call

Phone: +234 8028776685

Email: [john\\_alison444@yahoo.com](mailto:john_alison444@yahoo.com)

- Phishing
- Malware
- **Scam**
- None of the above

34) Scams can contain the following:

- Deals that sound too good to be true
- Alarmist messages and threats of account closures
- Promises of money for little or no effort
- **All of the above**

35) Which of the following is a/are not scam prevention tip(s)?

- If you should receive any kind of email which states "if you do not respond within 48 hours then your account will be suspended or closed" ignore them
- Before entering any personal information, make sure the website is secure
- **Verify account details when requested**
- All of the above



## Appendix E Unique Identifier List

Person ID	Pre-Assessment	Post-Assessment 1	Post-Assessment 2
1	KXV3IFA	VLRZUJC	ET4KAQD
2	S2GCEKD	W2EP6ZA	VLT4VIB
3	SDPUCLC	LLJWZPB	5CWAPQD
4	YC7GM3A	ETW9NZD	MBCFSBD
5	ZZ59ESD	GCPXRSA	AHQ5DFD
6	MCK34XB	XA4JNAA	TJZN3CB
7	ZBV6PNB	Q53L35B	AE5CALA
8	Y2UT9DD	5EKABSD	JSHCT3B
9	HIJ4MCA	LMLFSB	7IPVXFC
10	UQY4Y7B	9CFXNRD	PTW7VKD
11	2BFB9JB	D64VREA	TL9ABRB
12	YLVZ9JB	YU9N4NC	42JLP6D
13	SAWU3DC	FFJJ2LC	EZ2U76A
14	A6UFU3B	C25BHGC	6JC5DWC
15	XZ5IWJC	GVQI42A	GRXJR7B
16	6UZS7GA	DT3XNQD	BEBKP4D
17	ICYQKEB	ICPMYPD	4U5PGWD
18	V92PVJD	VNAZCIB	NSA45NA
19	DT7HPRC	PKET7YB	6G7PXGC
20	BBJ344D	9FJVCNB	R296TDD
21	T4ARHDA	EWSRCKA	BSTMS7B
22	4AW3VAB	5KTIJ4A	IIRGCBB
23	GGMPMKD	LDRQK7C	F5DCGLA
24	LG9XQIB	YMVSBKB	A2JN9MD
25	GRCMJYB	GAQ5CLD	QDRMCIB
26	93UQHGA	2LC3K6A	46L5S6B
27	S5VJDSC	22LXN6A	ACHFB9D
28	6UGUKLD	CDLDTTD	ZDW4F7A
29	3Z6PBCB	RLCDQXA	TJJKBBB
30	YKN3YJB	RLYK6DA	CBZZM7A
31	TDJXQZA	K4Y2QFC	ILATU2B
32	YRZYHHB	HXT2UAD	X4FXBRC
33	KFU74TA	H95Z44A	YUMUSHC
34	FHYLDFD	HIHAIWD	FWWVTKB
35	Q4Y7TBC	5KP2PZC	E6H4DSB
36	EHS9BGA	ARR6LPB	K4BDEMB
37	EKHWN4A	7QDIVVD	LAVQMNC
38	KG94T9D	7QQXYWA	WCK9B5B
39	9CMR5ID	5V3A5AB	T9JFXID
40	L2QSK6A	K59PMIB	LREGETA

A study regarding the effectiveness of game play as part of an  
information security awareness program for novices

---

41	6WG3MPB	93V9GIA	GWA9HHB
42	JMRSLRA	SU5F4EB	Y24WVZA
43	E9GKZGC	V2CKWVD	HU9TTQA
44	CAC7FSD	FBEH6TC	KX3CHGC
45	3KLH5MC	VW3FTKD	WE7TJQD
46	NIJENRA	MYYFQPA	9FG3UPC
47	A53RFZD	J476LEC	5DC6DCC
48	EVDWHQD	PBQDACD	F2BT5FD
49	D7DSC2D	CGZ4SXB	NAMGA6C

## Appendix F Consent Form

### Letter of informed consent to be signed by all respondents



**Research Project:**

Evaluating the effectiveness of a social networking site game to conduct a security awareness program to non Information Technology (IT) students within South Africa.

**Researcher:** Mr. W.A. Labuschagne / **Supervisor:** Prof. M.M. Eloff  
**School of Computing**  
**College of Science, Engineering and Technology**  
**University of South Africa**

Dear Prospective participant

I am conducting research for my MTech studies; I would like to request your participation in this study. The study is about determining the effectiveness of game play to enhance learning during a computer and information security awareness programs. Your participation will be during the completion of questionnaires or Internet usage as methods of collecting data. Questionnaires will be captured using web based or paper based surveys. Internet usage is defined as accessing a social networking site (Facebook) and playing a game to determine if learning is enhanced during game play. Data collected during questionnaires and Internet usage will remain confidential, but it can only be disposed after five years because of the university rules. After five years all material used in this interview will be destroyed.

Should you be willing to participant in this study; please complete and sign the section below

I \_\_\_\_\_ (full names of participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project. I understand that I am at liberty to withdraw from the project at any time, should I so desire. I hereby give permission that my responses may be used in the above research project, provided that none of my personal details will be made public in the published research report.

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**Place:** \_\_\_\_\_

## **Appendix G Published Papers**

All the papers listed in Section 9.5 follows next.

## The Effectiveness of Online Gaming as part of a Security Awareness Program

WA Labuschagne<sup>1</sup>, MM Eloff<sup>2</sup>

<sup>1</sup>School of Computing, University of South Africa (UNISA), Pretoria, South Africa

<sup>2</sup>Institute for Corporate Citizenship, University of South Africa (UNISA), Pretoria, South Africa

Aubrey.labuschagne@gmail.com

Eloffmm@unisa.ac.za

### Abstract:

Using cyberspace to conduct business and personal duties has become ubiquitous to an interconnected society. The use of information technology has provided humanity with a platform to evolve and contribute to the advancement of society. However duality also exists within the realm of cyberspace as shown by the expanding threats originating from cyber criminals who uses the information superhighway for nefarious purposes.

Companies usually invest large amounts of money in the implementation of hardware and software controls to deter and prevent attacks on assets within these establishments. For example firewalls and anti-virus software are updated as threats evolve. In spite of these controls the weakest link in this security chain is still the human element whose actions can be considered as erratic and unpredictable thus posing a threat to the security of the organization.

Security awareness programs aim to equip users of cyberspace with the necessary knowledge to identify and mitigate threats emanating from these platforms, including the Internet.

Numerous security awareness frameworks exist which prescribes the required steps to design and implement an efficient and effective security awareness program. An understanding of the different steps is required to develop and customize such a program for a specific environment. Furthermore different methods which include training, newsletters and websites are used to deliver the security awareness content to the participants. The nature of these methods could be ineffective and be considered mundane and strenuous to the participants who do not always have the technical background in information technology, which, in turn could threaten the success of the implemented program. Therefore a proficient solution should be considered to attract and captivate a diverse group of employees when doing security awareness training. Moreover the effectiveness of these programs should be measured with the application of metrics defined within security awareness programs.

This paper discusses the implementation and findings of a security awareness program. The aim of the security awareness program was to determine the effectiveness of using online gaming as an information security knowledge delivery method to enhance the efficacy of the participant's awareness to identify and mitigate threats encountered within cyberspace. Subsequently the paper proposes improvements to the design of the security awareness program used during the study.

**Keywords:** Security awareness, online gaming, effectiveness, education, metrics

### 1. Introduction

The Internet has penetrated all aspects of daily living within society. The speed in which technology has become part of normal day to day activities created a sense of panic as users attempt to understand on how to use these new technologies. The issue of using these technologies not the only concern as cyber criminals have turned to these to prey on unsuspecting users. The arsenal available to criminals is vast and very effective against users who unknowingly would engage in actions to their own detriment as they are not aware of the threats and how to mitigate these (Kim et al. 2011). An example is the use of social networking sites. Facebook has been widely adopted and used by users to keep in contact with friends. But the Facebook platform has also been used by criminals with great success as shown by the Koobface malware which infected 400,000 and 800,000 computers in 2010 (Villeneuve, Deibert & Rohozinski 2010). In another example Labuschagne demonstrated how social media sites could also be used to profile users based on comments and posts (Labuschagne, Eloff & Veerasamy 2012). In addition users have to learn about implementing security features on a computer to protect them from network threats, for example, using a firewall. Users without the

technical skills, struggle to adopt these security tools for several reasons including the user's technology adoption intention (Kumar, Mohan & Holowczak 2008). The use of a security awareness program equips computer users with knowledge to mitigate the threats that could be encountered on these platforms.

Many institutions have realized the impact of this and have started implementing awareness programs. Broadband Internet within schools in Taiwan achieved a 100% penetration in 2009. As a proactive measure by the Taiwan Ministry of Education, a security awareness program was launched to equip teachers with the necessary knowledge, whom in turn would transfer this knowledge to the scholars (Chou & Peng 2011). Computer security is defined as securing the platform from external threats and having peace of mind that the computer system is secured (Landwehr 2001). Security awareness would entail equipping users with knowledge to identify and mitigate external threats. In another way, it is defined as being exposed to knowledge about information security related content. This newly acquired knowledge would then in turn change future behaviour. Many companies implements security awareness programs to prepare their employees for the threats originating from the digital cyber world. Several frameworks exists which provide guidance in designing, developing and deploying security awareness programs. The European Union Agency for Network and Information Security (ENISA), the SANS Security Awareness Roadmap and the National Institute of Standards and Technology (NIST) framework were some of the existing frameworks that were analyzed to determine a solution for the security awareness program used in this study.

This paper discusses the implementation of a security awareness program to determine the effectiveness of online gaming as part of such a program. The first section of the paper provides a background on the different perspectives of security awareness programs; this is followed by a discussion of the security awareness program implemented at the University of Venda in South Africa. The analysis and findings are described next and the paper concludes with recommendations to Information Security Managers who plan to deploy a security awareness program.

## **2. Security Awareness Perspectives**

Security awareness programs can be designed and developed using existing frameworks. However many programs exist and the best suited framework should be selected to achieve the goals of increased security in the given domain. The ENISA framework is comprehensive and follows sequential phases which include individual steps to achieve the goal; however each phase must be completed first before continuing with the next phase. The first phase of the ENISA consists of 14 steps which includes numerous of meetings to determine the needs and identifying the goals to address the needs, selecting and recruiting a team and obtaining a budget. The second phase consists of 5 steps to execute and manage the awareness program. The last phase consists of 7 steps to evaluate and adjust the awareness program. Many of these steps require input and approval from stakeholder which potentially could increase the time to deliver the awareness program (ENISA 2010).

The SANS Security Awareness Roadmap provides an easy to interpret flow of objectives to be taken in order to implement an awareness program. This roadmap starts at no awareness program, then commences by developing an awareness program that is compliance and security metrics focussed but also promotes awareness and change resulting in long term sustainment. It provides a guide to what each objective entails and what the deliverable of each objective is. However the guide does not prescribe actions, hence additional research might be required by a novice who wants to implement a security awareness program (SANS 2010).

The NIST Awareness Framework provides enough detail to a novice to implement a security awareness program and also has been used in other studies related to security awareness programs. The NIST framework consists of four phases (Wilson & Hash 2003). The first phase entailed designing the awareness program by conducting a needs analysis. The participants of the study were students from the University of Venda. They used this security awareness program to enhance their skills as part of a community program to train people within rural areas on end user security. Another need was to determine what the current security awareness levels of the students were whom attended the awareness program. The second phase required the development of the program which included the material used during the execution of the program. The content had to address topics specific to threats end users might encounter within the cyberspace domain. The security awareness program was implemented in the third phase. This entailed identify methods to

effectively deliver the material to the participants of the awareness program. The framework implementation concludes with evaluation and feedback after the program was completed.

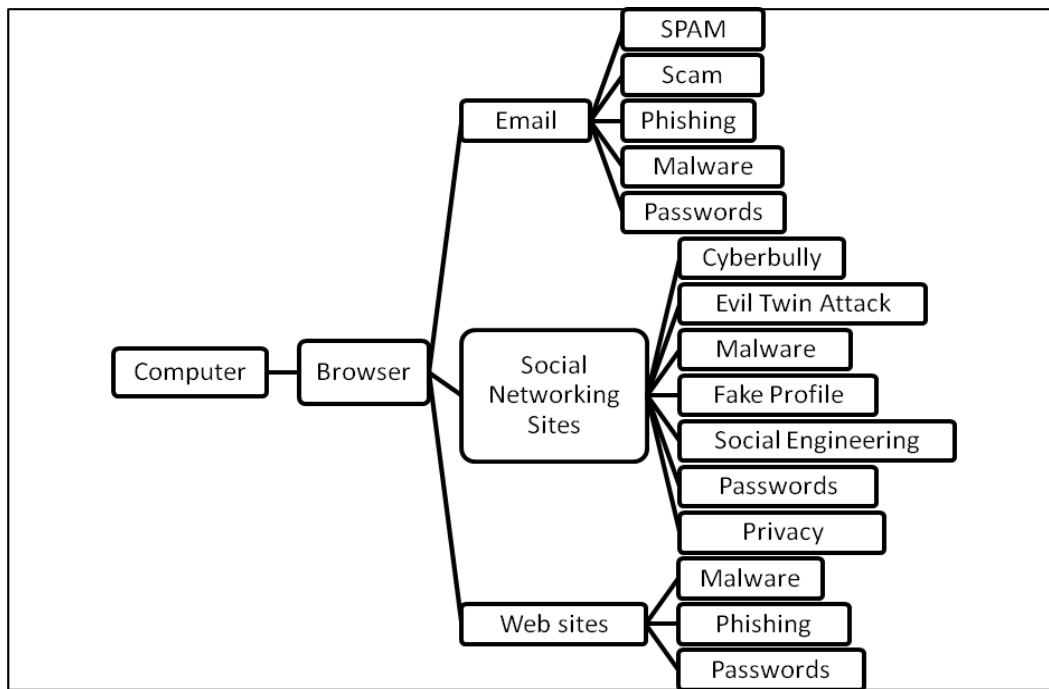
Several studies have shown the effectiveness of security awareness programs. Eminagaoglu, Ucar and Eren (2009) implemented a security awareness program which focused on password usage of 2900 employees at a Turkish company. Three password audits were conducted over a period of a year to measure the effectiveness of the program. The results indicated a significant decrease in the use of weak passwords. Dodge, Carver and Ferguson (2007) conducted a security awareness study on phishing attacks in the United States of America. They determined that the awareness levels increased over a two year period. They developed a system that delivered phishing attacks to students and measured how many fell prey to the attack. The results showed a decrease in successful attacks as the users become more aware of the threat. Another security awareness program was implemented at an international gold mining company which had offices in 11 countries that focussed on policies, passwords, email and Internet use, mobile devices and incident reporting (Kruger & Kearney 2006). The effectiveness of the study was measured by using multiple-choice questions provided to the participants, resulting as an indicator of awareness levels. The study also recommended that security awareness tools should consist of a broad set of questions covering the topics, using a practical system and it should be automated. These recommendations were considered during the design and development of the online game used within this study. A study conducted on the ever changing information security domain highlights the importance of the continual delivery of security awareness programs as a mechanism to equip computer users with knowledge to deal with cyber threats (Dlamini, Eloff & Eloff 2009). In other words, security awareness programs should not be a once off event as threats evolve with the rapid change in technology. This is supported by Rezgui and Marks who explored factors that effects security awareness (Rezgui & Marks 2008). They found that working environments does play a role and that iterated training should be regular to be effective.

Security awareness content is delivered using various methods including, but not limited to, posters, classroom-style training, websites and newsletters. Subsequently the effectiveness of security awareness programs also needs to be measured as this mechanism could improve future security awareness programs. A study conducted by Khan (2011) on the effectiveness of the different security awareness methods listed, group discussions and educational presentations are the most effective. Other methods, such as email messaging, newsletters, video games, computer-based training (CBT) and posters were not as effective when looking at knowledge gained, attitude to change, subjective norms, change in behaviour and a component of intention. However, video games have been used in security training as they draw the attention of the users and allow the users to implement knowledge acquired within a given scenario (Cone et al. 2007).

Most end users access services on the Internet using a web browser. The majority of users either access their email, social networking site accounts or visiting web sites. Subsequently types of attacks were associated with each vector also known as a vulnerability. The content of the security awareness program were designed to address each of the potential threats. The identification of the topics resulted from the development an attack tree by the authors to determine the different vectors that could be used with malicious intent against unsuspecting end users. The graphical representations of the different attack vectors are depicted in **Figure 1**.

The security awareness program discussed in this paper covered the following topics which subsumes the potential threats identified by the attack tree: Web Browsers, Passwords, Social Networking Sites, Cyber Bullying, Malware and Phishing.

The threats listed by the authors align with the threat landscape described by Veerasamy and Taute (2009) who conducted research in identifying what attack strategies and techniques were used against national, commercial, governmental and individual entities. The next section describes the implementation of the security awareness program.



**Figure 1:**End User Attack Tree

### 3. Method

The participants were from 3<sup>rd</sup> year Computer Science class at the University of Venda, Thohoyandou, South Africa, but also formed part of rural development plan to educate people from the area about the different security threats encountered within the digital realm. A class of 40 participants attended the security awareness program. All participants were in the same venue for the day session. The security awareness program was initiated with the first survey (Pre Assessment) which also resulted in determining the awareness level baseline of the participants. This was followed by a training session which covered security topics identified during the analysis. The training sessions did not exceed 15 minutes per topic as it was a precautionary measure against mental fatigue (Wilson & Korn 2007). A second survey (Post Assessment 1) followed the completion of the training session. The objective of the second survey was to determine if the training session had an impact on the overall security awareness levels of the group. The program continued with the participants playing a social networking game online. The game was designed and developed with gamification concepts in an attempt to improve the retention of the content from the topics discussed during the training session. Some of the design concepts included but was not limited to a leaderboard indicating who has attained the most points, a progressbar to provide a graphical feedback on how far the user was in completing the game and a timeline to provide all users with a view of other events that occurred within the game. A prize was handed over to the winner of the online game and the security awareness program was concluded with the final survey (Post Assessment 2). The objective of the last assessment was to identify if the online game had an effect on the awareness levels of the participants.

Data was collected during the completing of the surveys as well as playing the online game. The surveys were accessed online by the participants and consisted of seven sections with five questions per section which totalled to 35 questions per survey. Each survey was designed to address the same objective across the different surveys for example, to determine if the participant understood the concept of weak passwords. Access to the surveys were controlled with a unique token number and was individually issued to each participant.

The online game was hosted within Facebook and the objective required from the users was to acquire points by answering security awareness related questions which correlated with the topics used during the awareness program. Random events occurred within the game which could deduct points from the user's accumulated points. An example of such events was a virus infection or hard drive failure. Users could prevent losing points by obtaining an item which, once in possession, would counteract the event, for example, the

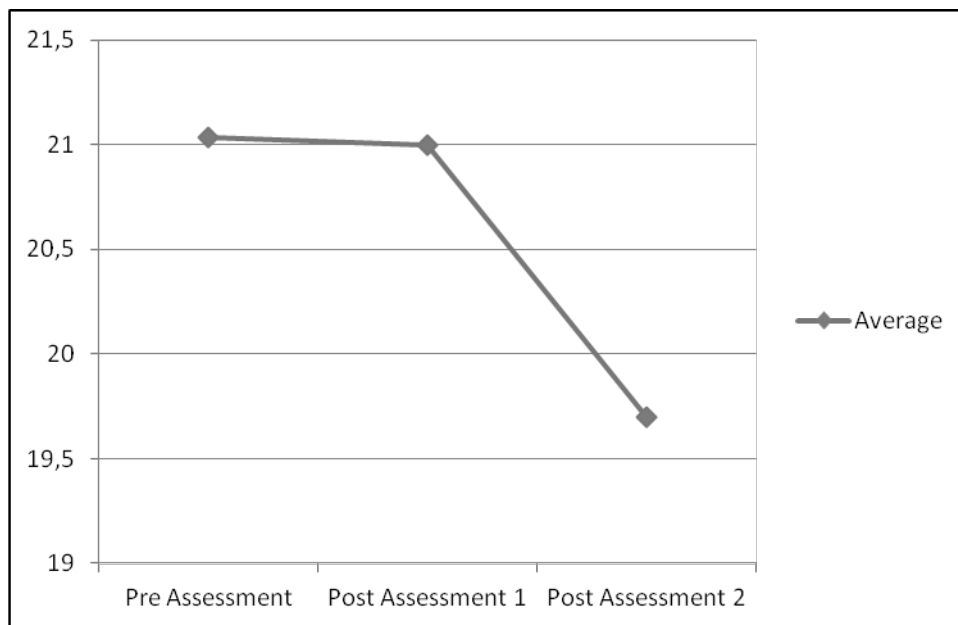


virus infection would be negated if the user has an anti-virus item. Users could buy items by using points accumulated hence losing some points in order to prevent a substantial loss of points when an event occur.

#### 4. Findings

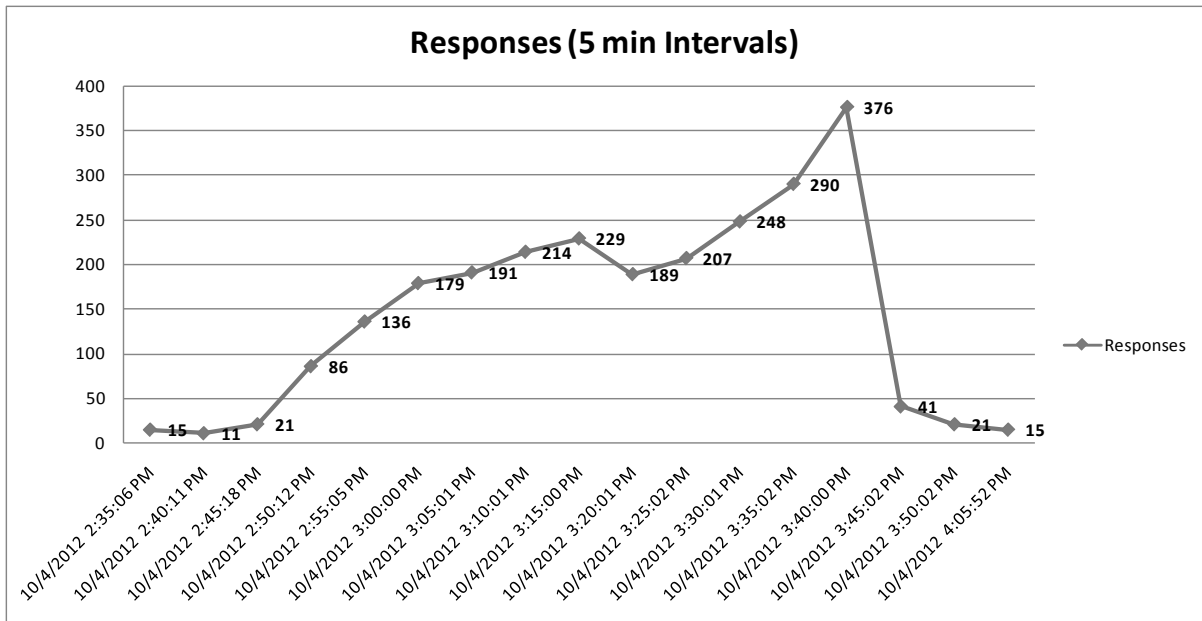
All the survey data was analyzed for each session and the results are depicted in **Figure 2**. Each item in the survey had a correct answer. Each participant's survey results were programmatically calculated to determine what topics each participant understood and what individual topics needs to be revised. This was seen as the awareness level of the individual. The group's awareness level was determined by averaging all the results of the group for each survey.

The first assessment which is used as the baseline shows the groups awareness levels at about 21 correct answers out of a possible 35. The participants then attended the training session which after the second assessment resulted in about the same number of correct answers as before the training session. Next the group participated in playing the online game that focused on the security awareness topics. The results of the third assessment after playing the game, show a considerable decline in correct answers. It was expected that the number of correct answers should have increased which would support the notion that playing the online game should increase the retention of the knowledge on the security awareness topics. Astoundingly the opposite happened and the awareness levels of the group decreased.



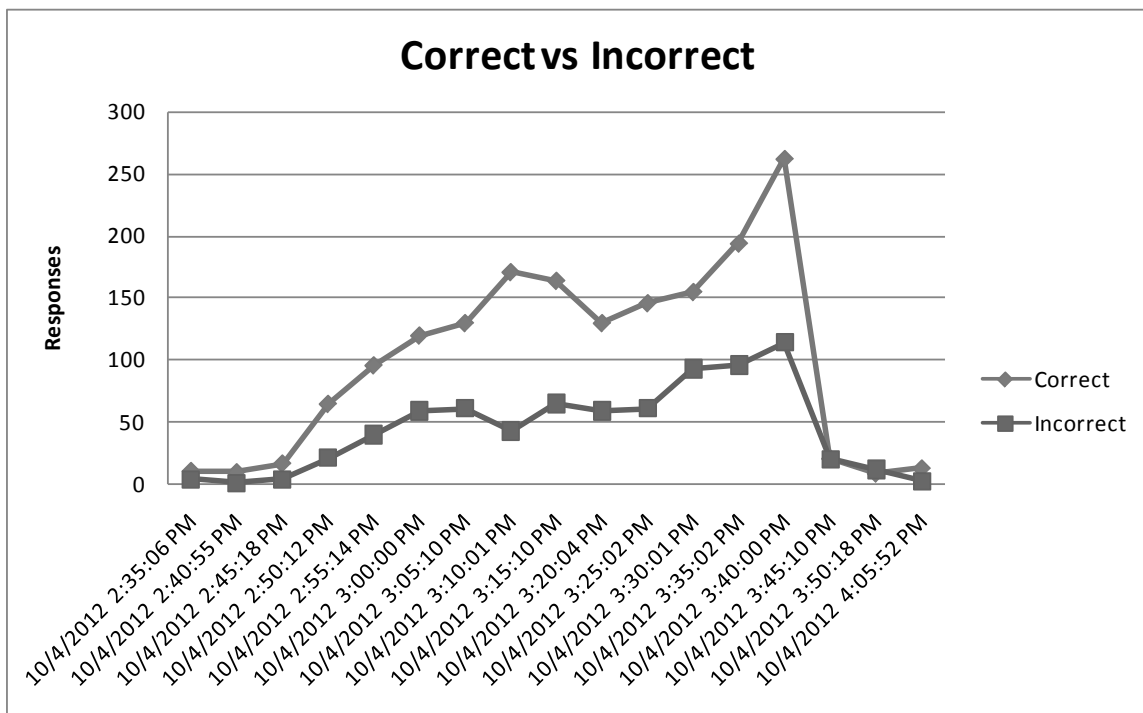
**Figure 2:**Session Averages

Next the online game data was analysed to determine if the results of the assessments are accurate in showing the negative effect of the online game on the group awareness levels. **Figure 3** shows the number of responses received during the playing of the game. Noticeable is the increase in responses as the deadline approached for the game play, which is mainly attributed by the prize which was handed to the participant with the most points.



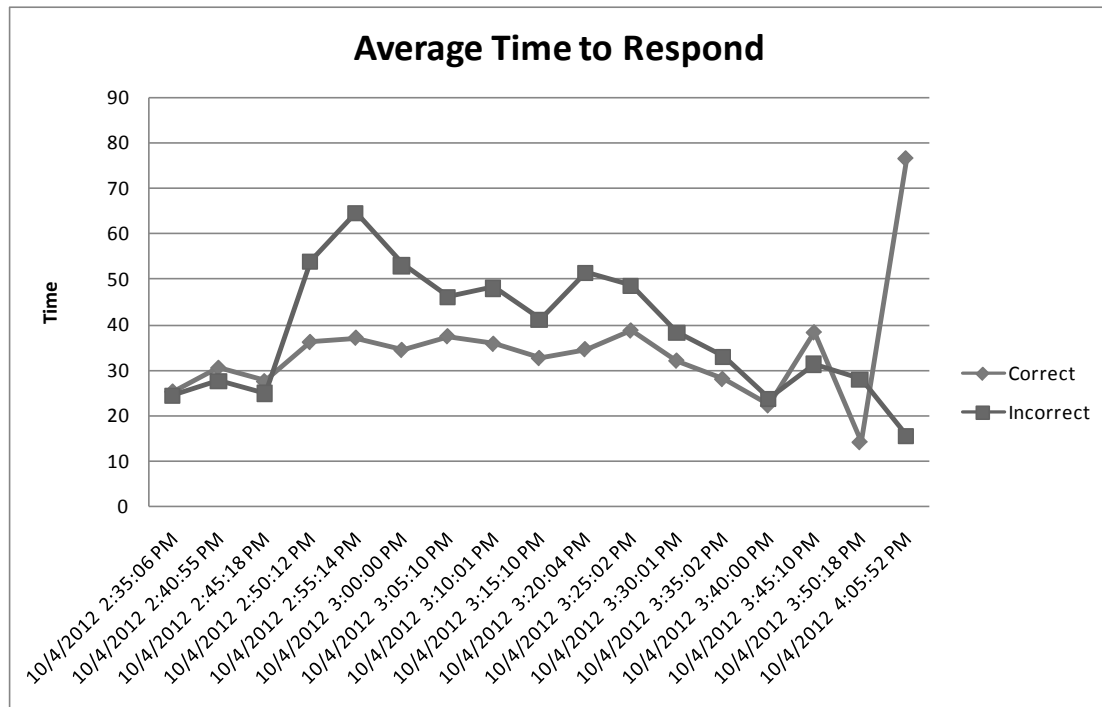
**Figure 3:** Average Response Time

The responses were classified to indicate how many were correct and incorrect (as depicted in **Figure 4**). Surprisingly the number of correct answers increased as the number of responses increased. This finding shows the participants knowledge on the awareness topics increased with time. Hence if the participants did not learn during the game play then the number of correct answers should have decreased and the number of incorrect answers should have increased. This could be due to the spacing effect as the recall of knowledge will decrease as time elapses. But the more the participants are exposed to the topic the longer they tend to remember it (De la Rouviere 2012).



**Figure 4:** Response Classification

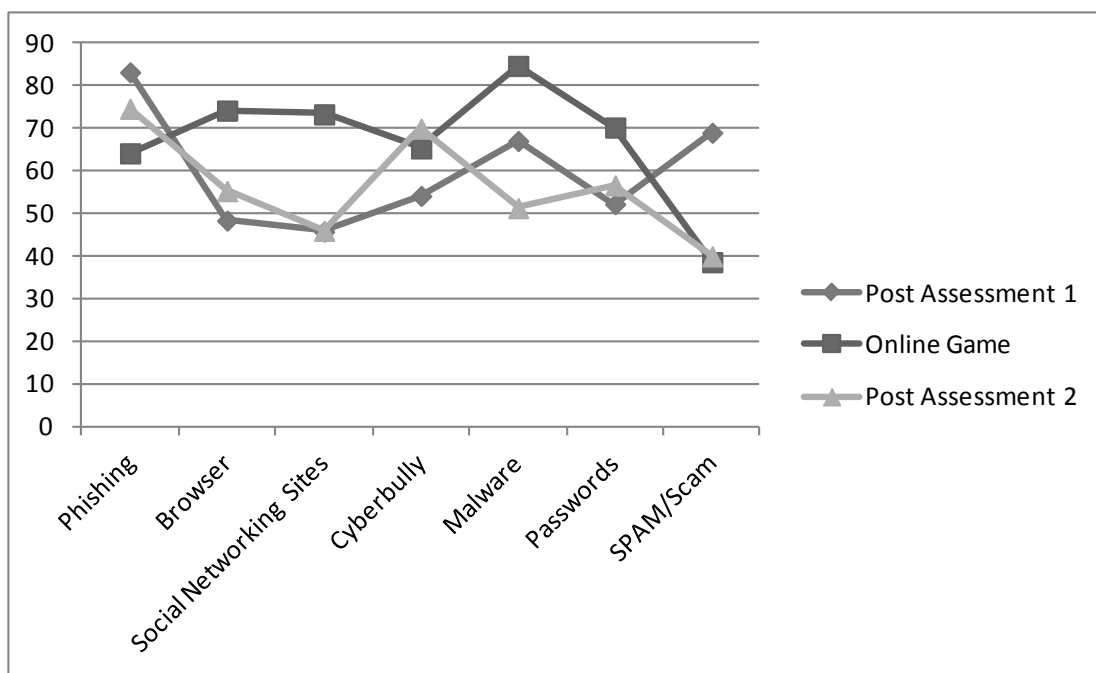
One of the metrics captured by the online game was the time it took for participants to read the question and then answer with the response. As the participants were in the same venue, the network latency affected all in the group the same way, therefore the response time calculations are consistent. An interesting observation shows that correct answers took a shorter time to answer than incorrect answers, even when more responses were submitted by the participants (See **Figure 5**). This also supports the notion that knowledge increased while playing the online game. Participants who did not know the answer had to consider the different options thus increasing the time to answer the questions. Participants, who had the knowledge, instinctively answered the questions quicker, hence a faster response time.



**Figure 5:** Average Response Time

Next the different topics answered in the online game were compared against the results from the second assessment (Post Assessment 1) and the last assessment (Post Assessment 2). The findings are depicted in **Figure 6**. The online game results show that all the topics except for Phishing and SPAM/Scam outperformed the individual topic results in the other assessments (Post Assessment 1 and 2). Also, if the online game had a positive effect on the awareness levels then the results of the last assessment (Post Assessment 2) should have improved against the results of the second assessment (Post Assessment 1). This was the finding except for Phishing, SPAM/Scam and malware however this is inconclusive in proving the positive effects of online gaming within this study however as discussed earlier the online game did indicate an increase in knowledge.

Alternatively the effect of the extrinsic motivation should be considered. The participants were competing for a prize as an incentive to partake in the study which was given after the completion of the online game. This would imply that the motivation for the students to partake in the study declined once the prize was handed over to the winner of the online game hence negatively affecting the results of the last assessment. This finding is aligned with results by Deci who examined the effect of extrinsic rewards on intrinsic motivation (Deci 1971). Subsequently the effects of the online game cannot be inferred due to the skewed results recorded during the last assessment.



**Figure 6:** Comparing Online Game with Assessments

## 5. Conclusion

Technology has become part of everyday living and society has embraced it as these digital platforms, which include mobile devices and the Internet, improves living conditions. For example many errands can be completed by merely logging into an Internet connected device and accessing services for example paying bills without leaving the comfort of their home. The duality of technology has become apparent as cyber criminals have seized the opportunity to use these platforms for nefarious purposes. Many users do not have the knowledge to identify these threats and mitigate it before harm is done. Security awareness programs are aimed at users who frequently use these digital platforms and to equip them with the appropriate knowledge to mitigate threats encountered within the cyberspace domain. Due to the nature of the computer domain, many users are not interested in the technical aspects as it is deemed complex and not interesting enough to engage the attention of the end user who is not technically inclined. This is detrimental to security awareness programs. These programs are delivered using various methods which include posters, training, presentations and websites. Games have been widely used to teach users about various topics as it is deemed fun. The use of games also provides a good indication if the user can implement new acquired knowledge within an environment. The effectiveness of games within security awareness programs was pursued in this study. The participant's security awareness levels were measured by using questionnaires that focussed on the different topics identified for the awareness program. The desired outcome of having an increase in the group awareness levels after the completion of the game play was not achieved. An investigation revealed that extrinsic rewards could have affected the intrinsic motivation which subsequently caused the participants to lose interest after game session. This subsequently meant the last questionnaire results which were critical in the study were affected. Thus it is the opinion of the authors that the final assessment (questionnaire) skews the results and cannot conclusively demonstrate that the gaming session can improve the security awareness levels of the participants. The study should be conducted again in future and only hand over the reward after the completion of the full program. However, analysis of the gaming session provided numerous findings that indicate learning has occurred. Participants substantially increased the number of responses as the session concluded, noticeably the correct responses increased as well. If the participants did not learn during the gaming session, then the incorrect responses would have increased. Another finding was the time for correct responses was shorter and consistent than incorrect responses which took longer. These findings provide feedback on improving future security awareness programs.

## 6. References

- Chou, C. & Peng, H. 2011, "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience", *The Internet and Higher Education*, vol. 14, no. 1, pp. 44-53.
- Cone, B.D., Irvine, C.E., Thompson, M.F. & Nguyen, T.D. 2007, "A video game for cyber security training and awareness", *Computers & Security*, vol. 26, no. 1, pp. 63-72.
- De la Rouviere, N. 2012, 30 Jan 2012-last update, How To: Learn Better by Learning Less. [Homepage of MIH Media Lab], [Online]. Available: <http://ml.sun.ac.za/2012/01/30/how-to-learn-better-by-learning-less/> [2013, 09/23].
- Deci, E.L. 1971, "Effects of externally mediated rewards on intrinsic motivation.", *Journal of personality and social psychology*, vol. 18, no. 1, pp. 105.
- Dlamini, M.T., Eloff, J.H.P. & Eloff, M.M. 2009, "Information security: The moving target", *Computers & Security*, vol. 28, no. 3-4, pp. 189-198.
- Dodge, R.C. 2007, "Phishing for user security awareness", *Computers & Security*, vol. 26, no. 1, pp. 73-80.
- Eminagaoglu, M., UÅşar, E. & Eren, S. 2009, "The positive outcomes of information security awareness training in companies-A case study", *Information Security Technical Report*, vol. 14, no. 4, pp. 223-229.
- ENISA 2010, *The new users' guide: How to raise information security awareness.*, European Network and Information Security Agency (ENISA).
- Khan, B., Alghathbar, K.S., Nabi, S.I. & Khan, M.K. 2011, "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, vol. 5, no. 26, pp. 10862-10868.
- Kim, W., Jeong, O., Kim, C. & So, J. 2011, "The dark side of the Internet: Attacks, costs and responses", *Information Systems*, vol. 36, no. 3, pp. 675-705.
- Kruger, H.A. & Kearney, W.D. 2006, "A prototype for assessing information security awareness", *Computers & Security*, vol. 25, no. 4, pp. 289-296.
- Kumar, N., Mohan, K. & Holowczak, R. 2008, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls", *Decision Support Systems*, vol. 46, no. 1, pp. 254-264.
- Labuschagne, W.A., Eloff, M.M. & Veerasamy, N. 2012, "The dark side of Web 2.0", *IFIP Advances in Information and Communication Technology*, vol. 386/2012, no. ICT Critical Infrastructure and Society, pp. 237-249.
- Landwehr, C.E. 2001, "Computer security", *International Journal of Information Security*, vol. 1, no. 1, pp. 3-13.
- Rezgui, Y. & Marks, A. 2008, "Information security awareness in higher education: An exploratory study", *Computers & Security*, vol. 27, no. 7-8, pp. 241-253.
- SANS 2010, *Security Awareness Roadmap*, SANS Institute.
- Veerasamy, N. & Taute, B. 2009, "Introduction to emerging threats and vulnerabilities to create user awareness", *Information Security South Africa (ISSA)*, Johannesburg, South Africa.
- Villeneuve, N., Deibert, R. & Rohozinski, R. 2010, *Koobface: Inside a crimeware network*, Munk School of Global Affairs.
- Wilson, K. & Korn, J.H. 2007, "Attention during lectures: Beyond ten minutes", *Teaching of Psychology*, vol. 34, no. 2, pp. 85-89.
- Wilson, M. & Hash, J. 2003, *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology, Gaithersburg.

# Determining Trust Factors of Social Networking Sites

Namosha Veerasamy and William Aubrey Labuschagne

Council for Scientific and Industrial Research, Pretoria, South Africa

[nveerasamy@csir.co.za](mailto:nveerasamy@csir.co.za)

[walabuschagne@csir.co.za](mailto:walabuschagne@csir.co.za)

**Abstract:** Social networking sites have become part of everyday use with many users posting updates of their status as well as establishing contacts. While many users use social networking sites to connect and maintain contact, attackers may see social networks as a prime target for spreading malware, propaganda or marketing. Many activities can thus be carried out using these platforms- both malicious and beneficial in nature. Social networking sites can be used for social engineering attacks as users may be eager to interact and engage with a new contact made on a social networking site. However, they may not be aware that the profile they are engaging with may be valid. In addition, malware is also being developed to target users of social networking sites. This paper entails the investigation of the reasons that users trust these sites. Users develop trust based on certain factors. Survey data is presented to indicate some of these trust factors. Users will also maintain a certain level of privacy based on the trust is established. Therefore, identifying why users trust social networking sites can be beneficial in understanding why certain information is divulged. Therefore, important questions that need to be answered are why do people trust these platforms and how much do users trust these platforms. These factors are important for security awareness to protect users from being attacked with social engineering techniques. Social engineering makes use of trust as a component to influence users to perform actions detrimental to themselves and others. In addition, this paper uses survey data to determine whether users are aware of these potential malicious objectives. Thereafter, the paper looks at the various indicators that could signal to users that they are not communicating with a genuine user but instead a fake profile. Another goal of this paper is to show users the dangers of social networking malware before they infect themselves. Once insight is gained into the trust factors, the study can also show users how social networking sites can be manipulated and thus help users protect themselves against being the target of attacks.

**Keywords:** trust factors, social networking sites, malware, profile, infection

---

## 1. Introduction

Social networks consist of nodes of individuals or groups with similar values, visions, goals, interests or friendships. Online social networks has helped encouraged such interactions due to its ability to rapidly share information and support communications. Online social networks allow users to create profiles that can be shared with contacts. A person's social status is often enhanced by their social profile. People are drawn together based on similar or shared social statuses. Thus, a social networking profile serves as an opportunity to grow a user's connections and thus expand one's contact circle.

Social networks have grown tremendously in popularity due to a number of useful features. This includes:

- Profile page showing details and interests
- Ability to connect to like-minded individuals
- List of contacts
- Photo albums
- Messages
- Status updates
- Comments
- Make new contacts
- Contact lookup
- Integrated applications, gadgets, add-ons

Due to the popularity of these sites, users may be eager to accept friend requests and posted links. Invitations may be easily accepted without any consideration of the consequences.

It is, however becoming vitally important that users be educated on the dangers of malware dispersal and fake personas. Social networking sites and the dangers of implicit trust have become a very important issue. Users need to made aware of the signs that perhaps that are not dealing with a legitimate user and how to evaluate

the various components of a social network account. Also when users seek information, it is often overlooked that people may turn to social networks of individuals to make trust decisions (Thomas, Enrico & Marian 2006). By assessing various components of a social networking site they will be better empowered to determine whether they are dealing with an authentic person or an automated account that may have malicious intent. The paper commences with a brief explanation of how trust in social networks is built. It then presents results from a survey polling users on their trust levels of social networks. It concludes with a model that summarises critical indicators that may arouse suspicion that users are dealing with an invalid profile.

## **2. Trust**

Trust grows when one party believes the other party will perform in such a way as to produce a positive outcome (Rahman, Haque & Khan 2011). Trust can also be established through a brand to deliver a product or service of a good quality. Trust helps build up an organisation's credibility, track record and thus helps develop a person's/organisation's reputation. Associated with trust is the aspect of privacy. Users also want to believe that social networks will protect their privacy and not divulge personal information. If users have a strong sense of trust they may recommend it to other users and will themselves continue using social networks.

A study was carried out by Nikolaos Volakis at the University of Edinburgh to investigate "Trust in Online Social Networks". A summary of his findings is given (Volakis 2011).

Trust looks at the relationships that people have, such that they place their trust in someone to behave in an expected way based on their previous behaviour. In social networks, trust often is determined by:

- Number of existing friends
- Number of messages sent
- Number of replies to the sent message
- Degree of influence on other users
- Position within a network of friends

Many people may form groups of interest to discuss a mutual topic. Thus, circles of trust may form in the group based on the topic of interest. A person who is not as knowledgeable on the topic may not be as influential as a hot avid fan or expert.

In an on-line environment, for trust to exist:

- The contacts should share a common background with regard to culture, topic or organisation
- The contacts should be certain of the other's identity.

These two points from Volakis can be argued in that a common culture, topic or organisation is not always possible. In other instances, people only find and form contact in a digital manner and thus there is no way to prove the other's identity. Thus, these points may not always be feasible. Furthermore, trust can be built based on reputation.

Critical to online trust is trustworthiness based on transparency and honesty. This paper entails the investigation of the reasons that users trust social networking sites. Users develop trust based on certain factors. Therefore, the next section looks at identifying signs why users should be suspicious of certain social networking accounts.

## **3. Identifying fake profiles**

Social engineering uses trust as a component to influence users to perform actions detrimental to themselves and others. There are various ways to carry out social engineering and influence users. One of these ways is the way a social network account is portrayed. The number of friends, types of photos and friends are all ways that can help create the impression of popularity. An automated account may also use abstract images. While there is no categorical manner to determine the validity of a social networking account there are various components of a profile that a user could evaluate to help indicate to them they should be suspicious. This section looks at possible signs that users may be dealing with an invalid social network profile. The initial discussion looks at evaluating profile pictures and pictures/albums on social network accounts.

Fake Facebook profiles often have (IdentifyfakeFacebook.com 2012):

- Have pornographic, attractive or related photos
- Profile Picture
- *Profiles with one profile pictures*
- *Profiles with no profile pictures*
- *Profiles with other profile pictures*



**Figure 1:** Images as profile pictures (IdentifyFakeFacebook.com 2012)



**Figure 2:** Provocative profile pictures (IdentifyFakeFacebook.com 2012)

A good indicator of a fake profile is thus the profile picture. Fake profiles may use pornographic, provocative or sexually orientated pictures as their profile pictures in order to attract people.

Another method of identifying a fake profile is the presence of a profile picture, which could be a photo of an attractive boy or girl, photos of actors or actresses.

A profile with no profile picture or random images could also be indicative of a false profile. However, some people may not use a profile picture or use the default pictures as they prefer not to display pictures of themselves. A better way to get a sense of a person is to look at their albums.

If a person uses pictures of professional models as their profile picture, it could be a sign of a fake profile. Other signs of fake profiles include (Hellbound bloggers 2012):

- Many male friends
- Many posts for requests for “Tag me!”. It is unusual if a person is tagged in various cartoon pictures rather than their own pictures
- Many applications requests like “Can you send me a chicken” or “Here a apple martini drink for you”
- In Facebook albums, fake profiles often have all their photos open to everyone. Other signs include:
  - *Really tiny photos*
  - *Many pictures but no tags indicating other profiles*
- Short profile- fake profile creators do not have time to create long and interesting profiles. However, a friend may have recently joined Facebook or is not very technology literate, and thus might have short profiles as they are still learning how to use the functionality.



***Namosha Veerasamy and William Aubrey Labuschagne***

- Many fake profiles have descriptions like “Accept my Farmville Request” or “Add me in Mafia Wars”. However, based on a conversation with a colleague about games/applications, one of them might send out an invite. In such cases, the request may be authentic.
- Conservative girls would not send requests to strangers. If a male receives random requests from girls, first verify the details (especially if the male is not particularly good-looking and the requests are from really attractive girls- this might be a way of tricking a person into accepting the request)
- The previous point also applies to females. Be wary of requests from very attractive males to average-looking females.
- Fake profiles may not have very frequent status updates. However, many users of Facebook are not very frequent users. They have created their accounts in order to get updates from friends and family around the world but rarely post anything about themselves. However, if their profiles are examined, there could be a legitimate profile picture, marital status, interests, a few family photos, etc. Their profile would appear legitimate without too many applications or tags.
- Many friends- On average fake profiles have 726 friends. If a person has an unusual profile picture (model, provocative or random image), does not update their status, only has friend’s add-ins as feeds, recently joined, has only cartoon pictures in their albums, has many tags on their photos, has many app requests and has hundreds of friends this is suspicious.

If a person joined recently and has many friends this could be suspicious. If a friend is in regular contact and they have communicated that they have just created a profile and send through an invite, this request could be trusted to be legitimate. However, random friend requests from people who joined recently, have models have profiles pictures and have many friends of one sex is slightly out of the ordinary.

Fake profiles can use lucrative pictures and catchy posts in order to attract more contacts. Individuals with a large and diverse network of contacts are thought to have more social capital than individuals with small, less diverse networks (Valenzuela, Park & Kee 2009). Spammers, marketers and attackers may then use this ploy to attract more users that can be used for their scams, product sales or attacks.

A few statistics based on fake and real profiles is given next in order to help identify fake profiles (Barracuda Labs 2012):

- Gender – 97% of Fake Facebook Profiles identify themselves as females
- 58% of females from fake profiles are interested in males and females
- 40% of real people claimed to have gone to a college versus 68% of fake profiles who make the same claim
- Fake profiles have an average of 136 tags for every four pictures whereas real people with profiles have on average 1 tag for every 4 photos
- 43% never update their status, compared to 15 % of real people that never update their status
- 35% of fake profiles lists entertainment interests

Users need to understand that spam can be sent out on social networking sites to lure them into phishing scams.

- Spear-phishing high ranking targets is called “whaling
- Spies set up a fake profile to lure a NATO official (Brean 2012)

Spam can also be used to market a specific company or product. It may be normal to like a clothing or food brand but be suspicious if a profile has constant support or posts about a particular company. Persuasion can consist of a number of influence processes, like those that increase awareness of a product or its features or change expectations about known features of the product (Aral 2011).

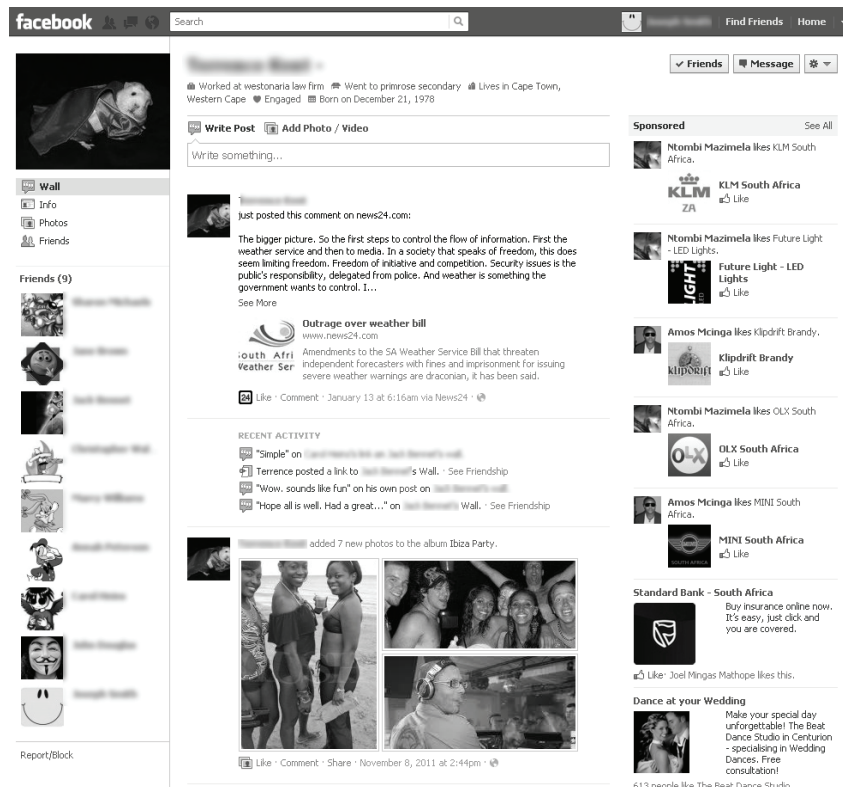
In essence, in order to determine where a contact is legitimate, study the profile. Sometimes a known contact is not very active on Facebook and therefore does not have regular status updates. They might have some photos showing their family and activities. A real profile is unlikely to have hundreds of tag requests to cartoon pictures. Users need to be careful of a profile with a provocative picture, is interested in males and females, has many friends, never updates status, excessively tags every photo, or has many app requests as there is a high probability it is fake

Others questions that may be asked to help identify fake profiles include (Facebook.com 2012):

- Are there pictures available of the person? Some people like to be private, but there is an option to show photos to friends.
- Is there constant blogs or posts about a company? Some people may like a particular brand of cold-drink or sportware but if a person constantly supports XYZ Incorporated, this could be a marketing ploy
- Has anyone ever met the person? If there are mutual friends, someone has had to have met the person. Mcknight et al explain the personal traits, structural assurance and normality of the Web, initial impressions and personal interactions play an important role for the formation of trust (Harrison McKnight, Cummings & Chervany 1998).
- Does the person make the same comments on multiple posts? This could be generic postings of spam messages or supportive comments in order to show interest in a profile. Is the only thing on their wall messages like “Looking good” on 10 different people’s accounts?
- Do they have a web site? The web site should be about them and not XYZ Incorporated.
- Do they make requests to support a prominent public figure but hide their identity? In such cases, the person just might be stirring trouble (especially if they remain hidden but prompt people to make controversial statements against well-known figures)
- Do they constantly take stabs at an opposition company?
- Some people may just pay compliments in order to get money. They will claim anything, including heart-breaking stories or even flirting. Evaluate carefully.
- Do they make meaningful comments or are they just giving a constant marketing or sales pitch?

People may choose to trust someone based on the past experience with the person or his friends, one’s opinion of actions taken by the person, psychological factors that are impacted by a lifetime of history and events, rumour, influence by others opinions and motives to profit amongst others (Golbeck 2005). However, users may choose to openly trust without being aware that they are dealing with an illegitimate profile.

In **Figure** an example of a fake profile is given. It has cartoon images as profile pictures as well as all their friends. There are no real albums and feeds are not meaningful.

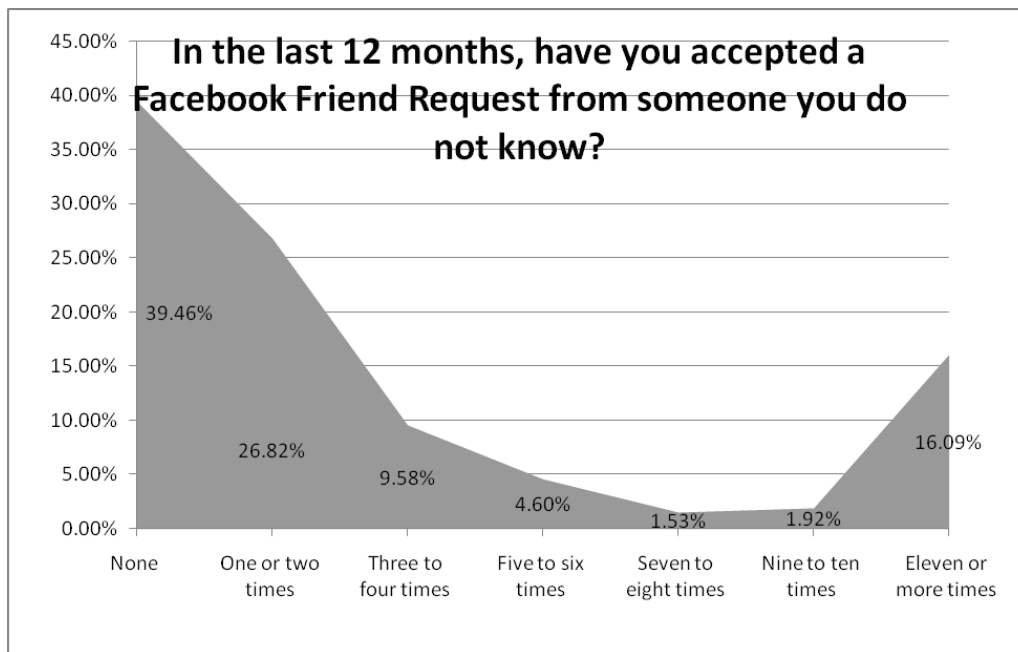


**Figure 3:** Fake profile

#### 4. Survey of trust factors

A research collaboration was undertaken with the University of Michigan in order to gain a more global perspective of the users' attitudes and views on security in the Information and Communication Technology (ICT) field. The survey contained questions relating to security in social networks. Some of the critical findings are presented in this section. There were 286 usable questionnaires. The data was collected over a period of six months in 2012.

The survey instrument included demographic questions. Some questions used a 5-point Likert answer scale from strongly disagree to strongly agree. The surveys were posted on-line and users were requested to complete the questions voluntarily. The survey participants included the following nationalities: South African, European, Namibian, Lesotho, Zimbabwean, Kenyan, Nigerian, Slovakian, Ugandan, and American. The majority of the respondents (61%) were male.



**Figure 3:** Acceptance of unknown friend requests

While 39.46% of users have never accepted a Friend request from an unknown contact, the rest of the responses are spread out across accepting such requests a few times to more than eleven times. This is alarming as users may not be aware of malware in social networks that send out random friend requests in order to make fake accounts appear more authentic. Koobface, a well-known Facebook malware has zombies that are required to find friends from existing accounts. Zombies would query the Command and Control server for logic credential to Facebook and would receive command like REG to register a new account or ADD, to log into an existing account (Thomas 2010). Fake accounts are then able to spam their list of contacts and spread more malware.

Participants of the survey were posed the question “Do you use privacy controls to protect your personal data on Facebook.” **Figure 4** shows the results. 73.18% of users utilise the privacy controls on Facebook whereas 12.64% of the respondents do not and 14.18% use them selectively. Even though the majority of the respondents did use the privacy settings, it is still an important message that users need to be made aware of the necessity of using privacy controls in order to prevent their sensitive information from viewed by any contact. With regards to fake profiles, if contacts are merely accepted, it will be possible for these contacts to gain a great deal of personal information. It is therefore imperative that users apply privacy controls in order to protect themselves.

**Table 1** shows the responses to the question “What personal data on Facebook has the most value for you?” One is the least valuable and six is the most valuable.”

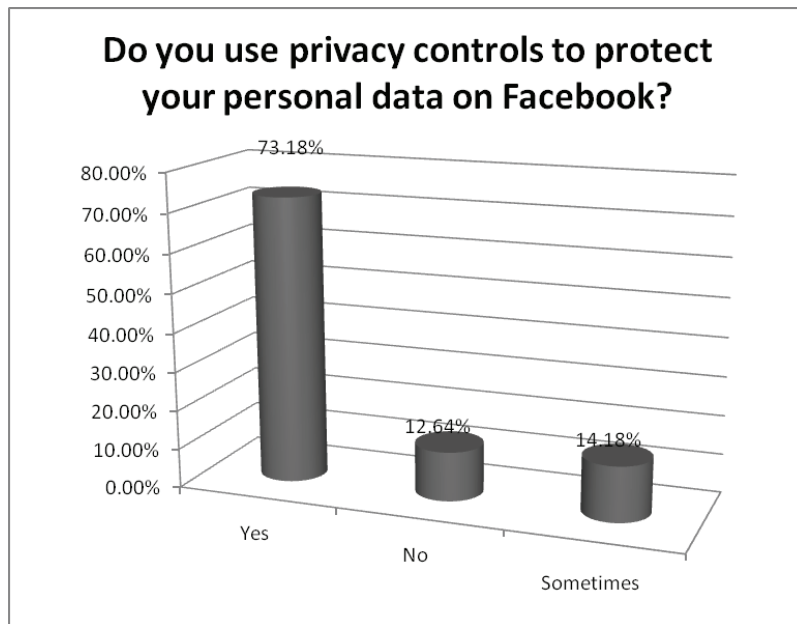


Figure 4: Use of privacy controls

Table 1: Response of question posed on value of personal data on Facebook

	Least valuable	Little Valuable	Not so Valuable	Valuable	Quite valuable	Most Valuable
List of Friends	21.84%	11.88%	18.39%	19.54%	12.26%	16.09%
Photos	6.51%	5.36%	11.11%	13.03%	21.07%	42.91%
Wall Posts	14.56%	9.20%	19.92%	16.09%	21.07%	19.16%
Contact Details	8.05%	7.66%	6.90%	8.43%	29.96%	59.00%
Interests and Activities	21.07%	19.54%	20.69%	14.94%	9.58%	14.18%
Messages	4.98%	3.07%	8.43%	11.49%	18.39%	53.64%

Repondants were asked to rate the value each of the components on a social networking account. The results show that feel that their contact details (eg. email, mobile number, etc) was the most valuable information to them (59% strongly agreed). 53.64% also rated messages as most valuable and 42.91% believed their photos had most value.

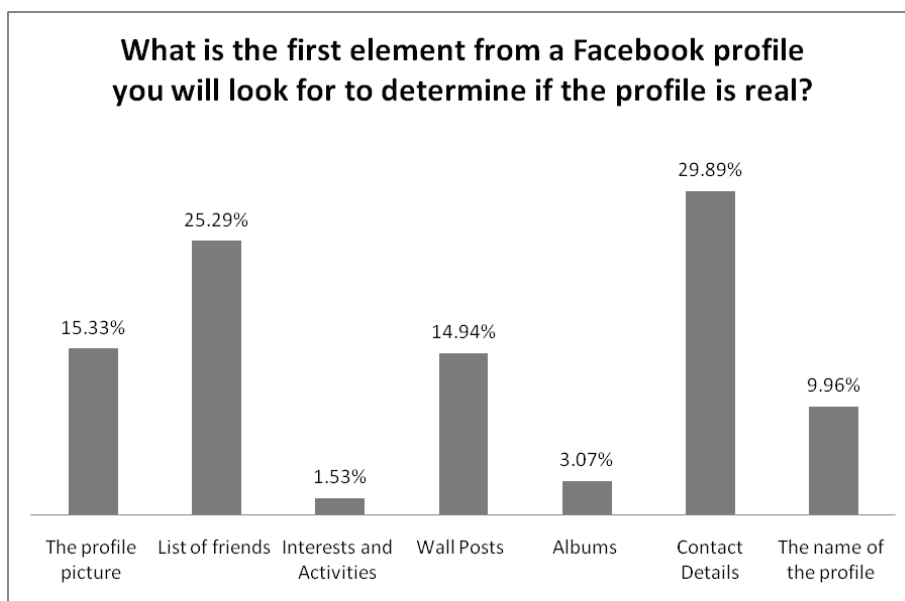
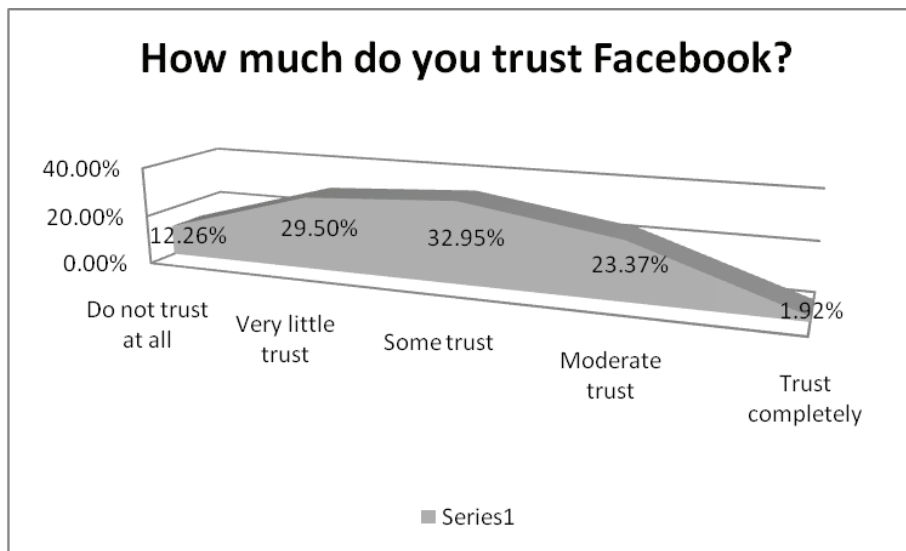


Figure 5: Determination of fake profiles

The response was widespread with regards to determining whether a profile is real ( **Figure 5**). The respondents mainly determined whether a Facebook profile was real based on the contact details provided (29.89%) or their list of friends (25.29%). However, 15.333% also looked at the profile picture and 14.94% would initially judge from the wall posts.

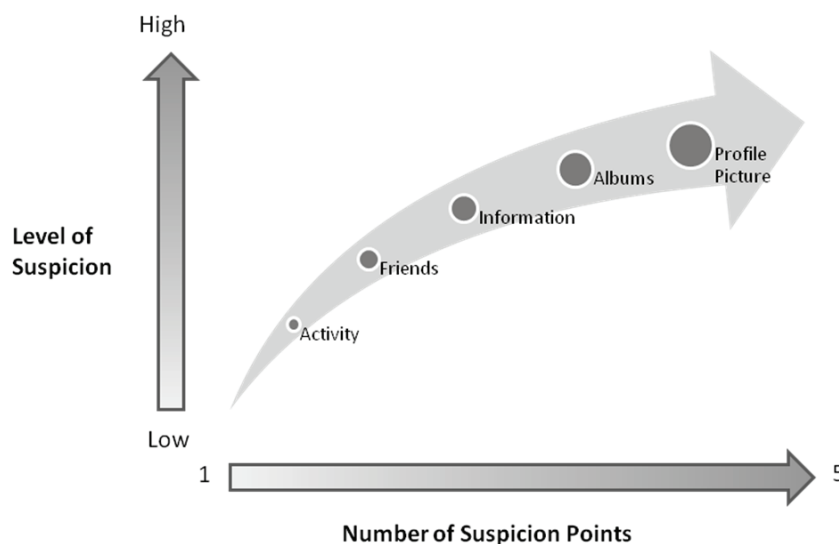


**Figure 6:** Trust in Facebook

The results concerning whether users trust Facebook was quite dispersed (**Figure 6**). The majority of respondents have some-to-moderate trust in Facebook with a very minor portion (1.92%) completely trusting Facebook.

## 5. Critical indicators

The previous sections describe some indicators that a social networking profile could not be genuine. Survey data was also presented concerning users' levels of trust concerning social networks. This section presents a summary model of the critical indicators that could alarm users of a suspicious social networking account.



**Figure 7:** Model of critical components to identify a suspicious profile

While it may not always be possible to determine the validity of social networking profile, the following components of a profile can be evaluated to indicate to a user whether they should be suspicious and exercise care. These include but are not limited to the timeline activity, friend's list, profile information, albums and the profile picture. These will be discussed in order of importance. **Figure 7** shows a summary of the critical components identified that can help a user determine whether a profile is valid.

The first component to evaluate is the activity on the user's timeline. The term timeline is synonymous with the term wall, and will be used interchangeably. This can be used to post information bits, which was visible to the user, as well as the friends. This information bits include but are not limited to interesting links, describing what they are doing, posting of pictures, commenting on other posts in the form of comments and adding personal information to their profile. The timeline could provide valuable information in the attempt to identify a fake profile. A timeline should be inspected for valid activities which indicates active creation of content, for example if a timeline contains a post about the user's plan for the weekend and a few of his friends make human-like comments on the post, then the legitimacy of profile increases. The activity on the wall is has the highest priority since many users who prefer anonymity might not post images or provide personal identifiable information, but still have an active timeline with legitimate content which indicate human interaction.

The friend's list should be examined next. Studies have shown that Facebook users have an average number of 130 friends, whereas many fake profiles have in excess of 600 friends (Barracuda labs, 2012). Not only the number but also the composition of the friends should be analyzed. For example, a fake Facebook profile might have a large number of men if the profile under investigation portrays an attractive female using sensual pictures.

Thereafter, the personal information associated with the profile can be examined. This information discloses gender, interests, activities, current location, education, real name, relationship status or date of birth. These are usually associated with real human beings. Although the absence of this information might raise suspicion, it should be noted that some users might withhold this information to protect their identity. The information provided should be logically analyzed for consistencies, for example if the data of birth indicates that the user of the profile is 18 years of age, then its unlikely that the user could be a doctor, worked in the banking sector for 5 years and have three children.

The albums of the profile should be inspected next. A real profile should have some pictures about the person. The legitimacy of the profile should be questioned, if the pictures contain non-human objects

or have pictures containing only one person. For example only having pictures without any other humans (friends) should be a concern, as well as having unrelated pictures uploaded. If the user has a high number of friends but does not have any images of friend interaction, then caution should be taken when contemplation becoming friends with this user. However, many users might not upload pictures to protect their privacy.

The last component of profiles that should be analyzed is the profile picture. Many fake profiles use provocative images to lure people of the opposite sex to accept friendship requests. Granted attractive people do exist but all the other components of a profile should be taken into consideration. Other users also use non-human images, for example a picture of nature or their favourite cartoon. These users protect their identity through obfuscation. A user should analyze all these components for consistencies before trusting the validity of the profile. Furthermore, social networking sites are used as a platform to promote socialization between users and lack of these components should be suspicious while the disclosure of these promotes trust. However, cognisance should be taken into consideration by looking at the information logically before implicitly trusting an unknown profile.

## **6. Conclusion**

The use of social networking sites has exploded with users making contacts and posting updates about their various daily activities. While many users use social networking sites to connect and maintain contact, attackers may see social networks as a prime target for spreading malware, propaganda or marketing. Many activities can thus be carried out using these platforms- both malicious and beneficial in nature. This paper describes various indicators to arouse suspicion that a social networking account make be fake. It provides survey data and a model to demonstrate to users their level of trust. This paper takes a very practical approach at educating users on how evaluate a profile to determine whether it is potentially fake.

## **References**

- Aral, S. 2011, "Commentary—Identifying Social Influence: A Comment on Opinion Leadership and Social Contagion in New Product Diffusion", *Marketing Science*, Vol. 30, no. 2, pp. 217-223.
- Barracuda Labs, Social Networking Analysis, [online], <http://www.barracudalabs.com/fbinfographic/>, Accessed 20120615.

***Namosha Veerasamy and William Aubrey Labuschagne***

- Brean J, (2012) [online], National Post, <http://news.nationalpost.com/2012/03/11/chinese-cyber-spies-set-up-fake-facebook-profile-to-friend-top-nato-officials/>.
- Facebook, How to Spot a Fake Profile, [online], <http://www.facebook.com/notes/my-social-practice/how-to-spot-a-fake-profile/199791076710071>, Accessed 20120615.
- Golbeck, J.A. (2005) "Computing And Applying Trust In Web-Based Social Networks", Dissertation Submitted to the Faculty of the Graduate School of the University of Maryland, College Park
- Harrison McKnight, D., Cummings, L. & Chervany, N. (1998), "Initial Trust Formation in New Organizational Relationships", *The Academy of Management Review*, Vol. 23, no. 3, pp. 473-490.
- Hellbound Bloggers, 10+ Tips To Identify Fake Profiles on Facebook, [online] <http://hellboundbloggers.com/2010/05/17/identify-fake-facebook-profiles/>, Accessed 20120615.
- IdentifyFakeFacebook.blogspot.com, How to Identify Fake Profiles on Face book, [online], <http://identifyfakeinfacebook.blogspot.com/>, 20101020.
- Rahman M, Haque M & Khan M, (2011) "The Influence of Privacy, Trust towards Online Social Networks: An Online Exploratory Study on Bangladeshi Customers Perception", *European Journal of Economics, Finance and Administrative Sciences*, ISSN 1450-2275, Issue 35.
- Thomas, H., Enrico, M. & Marian, P. (2006), "Person to person trust factors in word of mouth recommendation", Conference on Human Factors in Computing Systems (CHI '06). Montreal, Quebec, Canada, 2006.
- Valenzuela, S., Park, N. & Kee, K. (2009), "Is There Social Capital in a Social Network Site? Facebook Use and College Students' Life Satisfaction, Trust, and Participation", *Journal of Computer-Mediated Communication*, Vol. 14, no. 4, pp. 875-901.
- Volakis Nikolaos, (2011) "Trust in Online Social Networks", University of Edinburgh, School of Informatics, Master of Science dissertation, [online], <http://www.inf.ed.ac.uk/publications/thesis/online/IM110932.pdf>.

## **Dangers of Social Networking Sites- the Propagation of Malware**

WA Labuschagne, N Veerasamy  
Council for Scientific and Industrial Research, Pretoria, South Africa  
wlabuschagne@csir.co.za  
nveerasamy@csir.co.za

### **Abstract:**

Users sometimes lack the security knowledge to protect themselves whilst carrying out activities online. One of the most popular tools used online is social networking tools. The popularity of Facebook and Twitter has become exponential with users making regular posts and updates.

Due to the popularity of these sites, users easily engage and communicate with each other. Users may place personal details, hobbies and preferences in posts- all of which may look legitimate. Catchy phrases, controversial words and emotive language are all ways of enticing users into clicking on links. However, social networking site users may currently be unaware of the dangers, threats, attacks and malware that can stem from these popular forums. Malware, phishing attacks and digital attacks are emerging from these popular forums. The aim of this paper is to help users protect themselves against malware on the social networking platforms.

Various shifts in malware have taken place which include piggy- backing off files, email, spamming and now the instant messaging capabilities of social media sites provides an ideal avenue from which to dispense the next generation of malware which includes psychological tactics to influence users to perform undesired actions.

Users may seemingly be unaware that a simple click on a spam message or obfuscated uniform resource locator (URL) can be triggering the download of malicious malware that will command their computer to form part of botnets. It is therefore essential to create some awareness of these dangers and explore how users can protect themselves.

The paper will illustrate the dangers of social networking malware through examples. In addition, the paper will discuss propagation techniques used in social networking malware. The aim of the paper is to create user awareness to minimise the risk of falling prey to malware in popular social networking platforms. The paper will recommend best practices to users to guard against falling prey to social networking malware. In addition, the design of a high-level system to identify potential social network media malware will be proposed. Through this paper, users can better identify potential malware before they infect themselves.

**Keywords:** awareness, social networking sites, malware, propagation, social engineering

### **1. Introduction**

Social networking sites have increasingly been adopted by users to conduct various activities during the last few years. These sites allow like-minded people to connect and collaborate with other users. Each social networking platform is developed around a theme, for example LinkedIn is used for business relationships and to conduct job searches while Facebook is used to stay in touch with friends as well as making new friends. These platforms allow users to communicate with other users with communication features that include chatting and posting of messages. In 2012, the five major social networking sites were Facebook, Pinterest, Twitter, Google+ and LinkedIn (Larson 2012).

Although the uses of social networking sites have been advantageous from a social connectivity point of view, many disadvantages have been highlighted. For example, the Nielsen's survey in 2012 reported on the negative effects that social networking has on productivity within the workspace (McGarry 2012). They found that within the United States of America (USA) 121 billion minutes were spent on social networking sites between July 2011 and July 2012.

With the high uptake of social networking site by users around the globe another negative effect has taken form, the use of these platforms for nefarious purposes by cyber criminals. They use the laws of economics within the digital environment to make a profit by unleashing cyber attacks on potential victims on these popular platforms. Faghani describes social networking as consisting of high clusters of smaller networks with a degree distribution which could follow power law distribution, hence friends



of a user on Facebook could be very influential while others might not (Faghani, Saidi 2009). This implies the influential friends could help to propagate the malicious payload of cyber criminals quicker than other less influential friends. The sheer volume of users on social networking platforms would make money making endeavours worthwhile. Even a success rate of 1% within a target population of 1 million users is lucrative. In addition, the effort to reach the target population is minimal and cyber criminals have a wide choice of different vectors to use to attack these unsuspecting users. The attacks that could be used on social networking sites include but are not limited to SPAM, phishing, malware and identity theft.

An example of the propagation of malware through social networking sites took place in 2008. Facebook users started receiving messages on their walls instructing them to update the Adobe Flash plugin after clicking on the link to watch a movie in July 2008. The users who complied with the instruction were inadvertently infected with malware that resulted in unfavourable behaviours by their computers, including prevention of the infected computers to connect to Anti Virus (AV) vendors, as well as the modification of search results from search engines. The malware prevented AV's to update virus signatures that could be used to remove the malware from the infected system furthermore the users unknowingly visited web sites controlled by the attackers. More than 400 000 personal computers were infected by the social networking malware called Koobface (Protalinski 2012).

Users may seemingly be unaware that a simple click on a spam message or obfuscated uniform resource locator (URL) can be triggering the download of malicious malware that will control their computer from powerful Command and Control Centres forming part of botnets. It is therefore essential to create some awareness of these dangers and how users can protect themselves.

This paper addresses the various techniques of social network propagation, mitigation techniques and identification methods. A high-level system is proposed in order to help identify potential social network malware. The next section will describe social networking malware that has been encountered. The common propagation techniques will be identified by determining how the malware was spread between users.

## **2. Social Networking Malware**

Facebook is a social networking platform where malware can be used to propagate and infect unsuspecting users. Bradbury listed attack vectors that could be used from Facebook. These attacks include but are not limited to clickjacking, click fraud, survey scams and rogue apps (Bradbury 2012). The following social networking malware will be analysed to determine what techniques were used by cyber criminals to ensure they became viral and spread amongst users:

- **Koobface**

Koobface is a well-known bot that utilised social networking sites including Facebook, Twitter and MySpace to propagate (Villeneuve, Deibert & Rohozinski 2010). The main mode of operation was to automatically spam numerous users with a catchy phrase and therefore entice users to click on the embedded link. Cyber criminals would hide the malicious looking URL with the use of short URL services that could include bit.ly (Baltazar, Costoya & Flores 2009). For example, [www.malcioussite.com](http://www.malcioussite.com) would become <http://bit.ly/YemU4W>, hence the user would not know where the final destination of the link would be. The obfuscated link would prompt users to upgrade their Flash Player or Adobe Acrobat. If users clicked on the malicious link, malware would be installed on the user's computer.

- **Most Hilarious Video Ever**

On May 29 2010, posts were made prompting users to click on a link to the "Most Hilarious Video Ever" (Runald 2010). Due to the title of the posts, various users were convinced to click on the link. When the user clicked on the link it took them to a spoofed Facebook page. Eager to view the video, users entered their credentials on the fake Facebook login page where their credentials were captured. Victims of the attack had their credentials captured and many of their accounts were compromised (Arthur 2010).

- **Strauss-Kahn Video**

In June 2011, a new attack surfaced on Facebook. The headline contained carefully constructed words to draw the attention of the reader and it also included a provocative image

to lure users to click on the link to view the x-rated video clip (McMillan 2011). The video clip allegedly contained content depicting disgraced Strauss-Kahn, a former International Monetary Fund (IMF) Managing Director, and a hotel maid. The headline and graphical photo appeared as part of a news feed on Facebook. It was in the format of a video link that a friend had liked (Smith 2011).

- **Rihanna and Hayden Panettiere**

The Rihanna and Hayden Panettiere video was another version of the Strauss-Kahn Video whereby celebrities were used as part of a ploy to draw users' attention to the post containing explicit content (Cluley 2011). This attack started in June 2011. The attackers created their attack using two components to draw users to the malicious content. First using two well-known television celebrities Rihanna and Hayden Panettiere (who are well-known to most users) and secondly adding a sexual context.

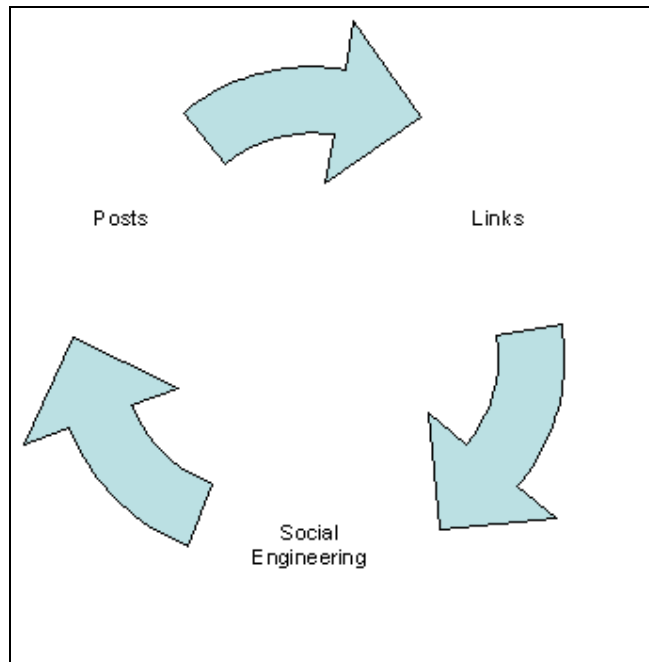
- **Syrian Activists Phishing Attack**

Various Syrian opposition activists have been targeted by phishing attacks that attempt to steal their YouTube and Facebook login credentials. Some of the attacks install malicious surveillance software on the victims' devices. One of the attacks stemmed from a link posed in the comments section of Facebook pages of leading Syrian opposition members including Burhan Ghalioun, Chairman of the Syrian Opposition Transitional Council. After clicking on the link in the comments section, a page was displayed that had the appearance of a Facebook security download application. If the user clicked on the download, they were actually installing a malicious keylogger that collected key strokes made by the user (Galperin, Marquis-Boire 2012).

This section discussed the various methods that social network malware can be propagated. The next section addresses the identification of social networking malware components.

### 3. Social Networking Malware Components

Table 1 lists the findings of the analysis of social networking malware. The analysis was categorised using posts, links and social engineering. These three components as depicted in Figure 1 are highly effective on social networking sites as these platforms uses these to ensure a social experience.



**Figure 1: Effective Components for Propagation**

The cyber criminals used the message-posting feature on Facebook to spread the dangerous payload. In Facebook, all users have a timeline where messages are posted. These messages are visible to all the other users who have access to the victim's timeline. The newsfeed will typically broadcast the message to all the users.

Malware cannot be deployed directly on a social networking site. Cyber criminals need to deploy the malware on external locations and subsequently create a link from the social networking site to the location of the malware. With the malware deployed, the next step is to ensure that users are lured to the message; this is achievable using attention grabbing content that include enticing images and provocative text. Social networking malware cannot execute by themselves and require the user to activate it (Provos et al. 2007). For example, the user needs to click on a link to view the video clip. Social engineering is used by cyber criminals, which influences users to perform actions that they would not under normal circumstances have performed (Hadnagy 2010). Grandjean noted common social engineering ploys used by malware writers including pornographic links and images, fake emails from financial services, threatening emails, urgent news and celebrity misbehaviour (Grandjean 2008). All the analysed social networking malware have similarities in that each of them posted a message on the timeline of unsuspecting users. In addition, a user had to click on the link to be directed to the malicious site with the malware and finally all of them used social engineering tactics.

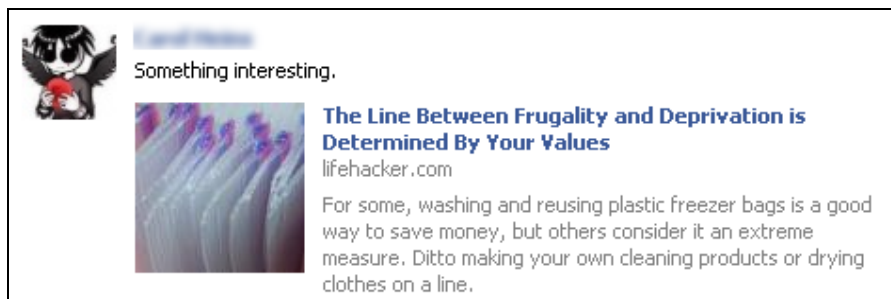
**Table 1: Social Networking Malware Propagation Techniques**

Name	Post	Links	Social Engineering
Koobface	Yes	Yes	Yes
Most Hilarious Video Ever	Yes	Yes	Yes
Strauss-Kahn Video	Yes	Yes	Yes
Rihanna and Hayden Panettiere Video	Yes	Yes	Yes
Syrian Activists Phishing Attack	Yes	Yes	Yes

As a result, from the analysis of the mentioned social networking malware the common three components used are posts, links and social engineering. Kritzingner and von Solms state the vulnerability of personal Internet users is due to the fact that they lack the information security knowledge to understand and protect their personal computers and therefore also their personal information (Kritzingner, von Solms 2010). Next, the three components will be described within the context of messaging on Facebook.

#### 4. Facebook Messaging

A Facebook message contains at most three elements which can be described as the text, an image and a link to an external web resource for example a web page as depicted in Figure 2. Figure 3 illustrates clearly the different components found within a Facebook message.



**Figure 2: Facebook Message**



**Figure 3: Facebook Message High Level Design**

This implies a Facebook message will always have at least a text element. The other elements can be added to draw the reader's attention with the use of images and also be more useful with the use of links to web sites which contain further information. The textual data provides no visual cues but does describe the context of the textual data. An image provides a graphical cue that users can use to infer the context of the message. The link provides the user with a mechanism to visit an external web site, which could contain more information. For example in normal circumstances a message ( such as "Samsung released new Galaxy phones with new design and features") might be posted by a Facebook friend about an interesting article that was read about the new smart phones that are currently rolled out. . A user who reads this message should be able to infer the context of the posted message. The timeline where the message will be visible will compete with other posted messages and could be missed since it is competing for the user's attention. A user who posted the message could add an image of the new design of the afore-mentioned smart phone to draw the attention of the user. This will make the message more prominent and increase the chance of it being spotted by other reading users. The posting user could then also add a link to an external web site that provides more information on the new smart phones.

Figure 4 is an example of a malicious message posted on Facebook. All three components are present. Provocative images together with enticing text are used within a post to draw the attention on the user, an obfuscated external link to watch a video clip of a well-known celebrity. This message will also be posted on the timeline hence all the other unsuspecting users will see the message. If the user clicks on the link, they would be instructed to download software to watch the video clip. The software is malware and infects the web browser to ultimately spread the worm to other Facebook users (Corrons 2012).



**Figure 4: Malicious Message**

The next section addresses how security vendors are addressing the threat originating from social networking malware that uses links to propagate and infect other computer systems.

## 5. Security Measures

End users who do not have the required security knowledge have a high possibility to fall victim to social networking malware attacks. Cyber criminals are aware that users on social networking sites trust these sites implicitly and many examples in recent times have shown that users befriend strangers on these platforms without verifying the identity of the other users (Labuschagne et al, 2012). The Internet is faceless which implies that a user does not know with whom he is really communicating. Merely receiving a message from a friend on a social networking site does not imply that one can trust the content of the message. Humans are social beings and cyber criminals exploit these traits by designing attacks that focus on their curiosity. For example, the death of a celebrity drives users on the Internet to read articles covering the story. Cyber criminals have used celebrities to lure unsuspecting users to malicious websites and subsequently infect their systems with malware. Users receiving a message on social networking sites should ask the following questions before proceeding and clicking on the link:

- Does the message evoke an emotion (curiosity)?
- Does the user trust the origin of the message?
- What action does the message require the user to complete?
- Is the message a hoax, this can be determined by visiting sites which lists the latest hoaxes for example [www.hoax-slayer.com](http://www.hoax-slayer.com)?

These questions are used to assist in the decision making process before the user proceeds by clicking on the link. The users have control over the situation by positively answering these questions.

Social networking malware is innocuous and only becomes a threat once the user activates it. The major threat resides with the payload that the victim needs to trigger by executing it after downloading the malware from the malicious website. Security vendors have implemented mechanisms to warn and prevent users from accessing the malicious websites. For example, website reputation services can be used to scan URLs for malicious content.

Angai analysed the effectiveness of Safe Browsing Services in 2010 (Angai et al. 2010). They used Norton Safe Web, McAfee SiteAdvisor and Google Safe Browsing services to determine how effective website reputation services are in identifying malicious websites. They found that these services are inadequate in protecting normal users when only one service is used; they suggested a more effective solution be the use of more than one website reputation services.

These results are supported by another study conducted by StopTheHacker.com (Jaal LLC) (Anonymous2010). This involved the testing of 721 URLs to determine the accuracy of website reputation service and identify the convergence in terms of safe/unsafe website. These tests included using the following website reputation services: McAfee SiteAdvisor, Norton Safe Web, Google Safe Browsing, Microsoft Bing and Comodo SiteInspector. The study concluded that the effective detection rate is not sufficient to allow users to implicitly trust these services. These services utilise different methods for analysing URLs in the identification of malicious sites. Due to different implementations, these website reputation services vendors use different databases to store the data about the malicious sites, thus causing inconsistency between different sets of data from the different website reputation services. In addition, the size of the Internet makes the process of scanning all the available URLs within the Internet a cumbersome process. Furthermore cyber criminals create new malicious URLs every minute (Anonymous2011) hence it is impossible to have a list of all the malicious URLs on the Internet since these newly created URLs must be reported as suspicious and then analysed for malware.

In some cases some URLs might be wrongly identified as malicious. The website reputation services will only be evoked when the user clicks on the link. This clearly shows the need for a more comprehensive solution that would prevent the user from clicking on the link. Next, a system is proposed to provide a holistic solution in addressing the propagation of social networking malware using social engineering tactics.

## 6. Proposed System Description

The proposed system consists of different components that will be used to look at each of the potential vectors individually and present the user with an early warning system. The system will analyse the context of the posted message by predicting if it is a social engineering attack tricking users to click on a link. Each of the individual components will be analysed to determine if they

together form part of a social engineering attack. The different possible combinations are listed in Table 2.

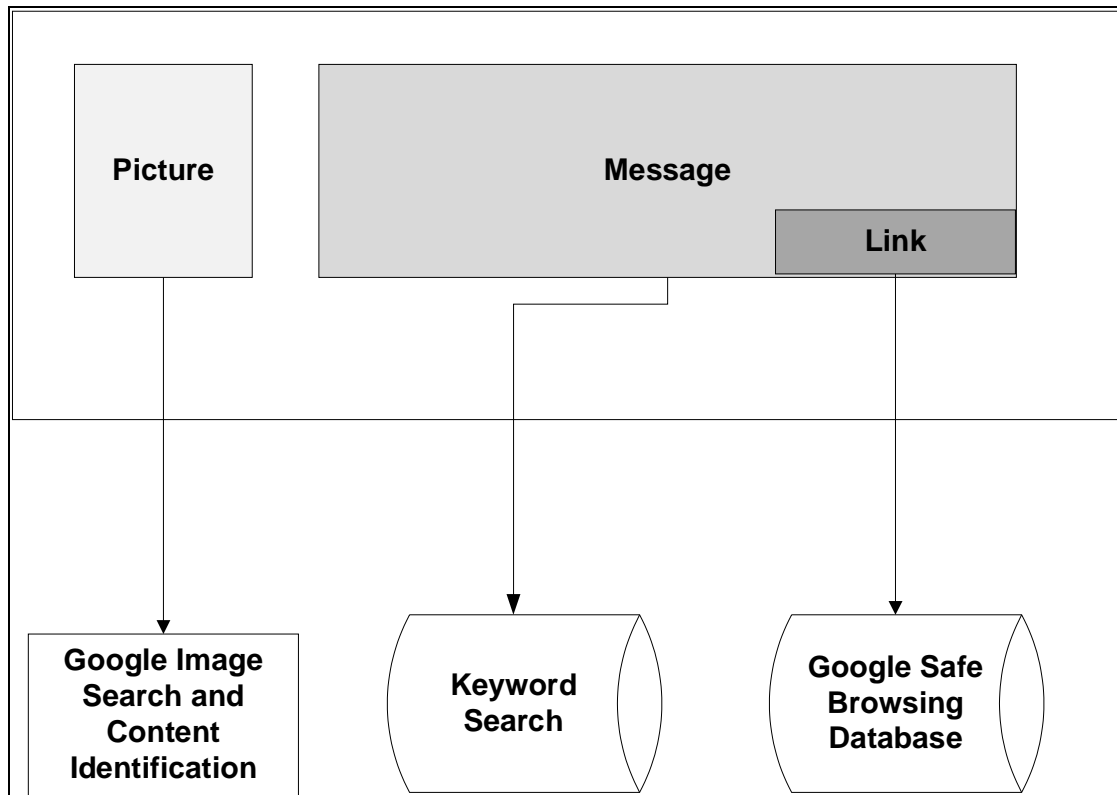
**Table 2: Warning System Table**

Text (Message)	Picture (Image)	Link	Threat Rating
No	No	Yes	Medium
No	Yes	Yes	High
Yes	Yes	Yes	High
Yes	No	No	Low
Yes	Yes	No	Low
Yes	No	Yes	High

In the event that only the link is available then the link will be analyzed in isolation. This would also be categorised as a medium threat since social engineering attacks would use all three components to be most effective. If the message contains a link then the system will also need to analyse the other components, if they are present. The text in the message will be tested to determine if it contains words which could draw attention for example the use of attention words like “OMG”, “Shocking”, “WOW”, “Revealing”, “Latest news”, “sex”, “pornography”, “naked”, etc. The link will also be analysed to determine if it has been identified as a malicious link using a website reputation service called Google Safe Browsing (GSB). A message containing a link and text containing attention words would be classified as a high potential threat. If the message contains a picture, then analyses of the picture is required to identify the theme of the picture. If the theme of the picture is classified as enticing or provocative together with the presence of a link in the message, then the message is classified as a high potential threat.

It is a possibility that a user posted a message that contains an enticing picture and a link to a site containing adult content. Even so, many of these adults’ sites as reported by Wondracek, contain malware which could attack unsuspecting users visiting these sites and these users should be warned about the potential danger (Wondracek et al. 2010). Therefore, if the message contains an enticing picture, attention words and a link then users would be made aware of the potential danger of a social engineering attack. The system would provide the user with appropriate notifications to prevent them from performing undesired actions, which could put the users’ security at risk for example downloading software to watch an online video. A message containing no links is considered as safe or no threat even if the picture is marked as enticing and if the text in the message contains attention words. The threat exists when a link is present which could link to malware.

At an implementation level, different technologies could be implemented to analyse each of the different components as depicted in Figure 5. The textual analysis would be conducted using keyword frequency analysis to determine if certain attention words are present within the message. GSB could be used to analyze the links to determine if they have been classified as malicious. The implementation of GSB does have effects, which should be considered. For example all the black listed web sites are stored in a database. The location of the database determines how quickly the analyses will occur. Also, the location will also affect how up to date the database data will be. Two choices are available when using GSB, download the entire database with all the blacklisted websites or use the application programming interface (API) to connect to the online database (Kuo et al. 2005). Furthermore, analysis is required to determine what theme is depicted in the image (Yee et al. 2003). The result should consist of a threat rating which could identify potential social engineering attacks and inform the user of a suggested action before clicking on the link.



**Figure 5: High Level System Description**

## 7. Future Work

The development and deployment of the proposed system will be pursued as future work. The complete system will be developed first to test the conceptual idea subsequent work will be focused on the optimization and effectiveness of each individual component. In addition, security awareness content will be created which addresses the issues of social engineering malware and how the propagation of these could be mitigated on social networking sites.

## 8. Conclusion

Social networking sites have been widely adopted as part of everyday life, which include staying in contact with friends but also conducting business. Duality also exists within the social networking domain whereby cyber criminals are using these platforms to attack users for nefarious purposes. Due to the nature of social networking sites that promotes sociability, many cyber attacks have incorporated social engineering into their arsenals. Many examples of successful social networking malware has been reported during the past few years where Koobface was the most profitable for cyber criminals but also very effective. These social networking malware uses specially crafted messages posted on the users' profile. The messages entice users to perform undesired actions for example clicking on a link to view a video and then unknowingly install malware that infects their computer systems and opens themselves to many other attacks. These messages contain three components: a link to an external web site, pictures and text to draw the attention of the inquisitive user.

Website reputation services do exist which can be used to analyze the link but studies have shown that at the current time these are not as effective-hence the user should be prevented from clicking on the link. User's attention should be drawn to these links with the use of text and images. These components should also be analyzed to determine if the message contains social engineering tactics and inform the user about the potential threat. A high-level system design is proposed to address

each of these components as a social engineering prevention system to mitigate the threat of social engineering malware on social networking sites.

## References

- Security Threat Report* (2011). Available: <http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf> [2013, 02/15].
- Website-Reputation Services Agree to Disagree* (2010), 2010, 17 January-last update [Homepage of StoptheHacker], [Online]. Available: <https://www.stopthehacker.com/2010/01/17/website-reputation-services-agree-to-disagree/> [2013, 01/15].
- Angai, F., Ching, C., Ng, I. & Smith, C. (2010), "Analysis on the Effectiveness of Safe Browsing Services", .
- Arthur, C. (2010), *Twitter 'funniest video' link hides malware threat* [Homepage of guardian.co.uk], [Online]. Available: <http://www.guardian.co.uk/technology/blog/2010/may/20/twitter-funniest-video-security-threat-malware> [2013, 01/27].
- Baltazar, J., Costoya, J. & Flores, R. (2009), "The real face of Koobface: The largest web 2.0 botnet explained", *Trend Micro Research*, vol. 5, no. 9, pp. 10.
- Bradbury, D. (2012), "Spreading fear on Facebook", *Network Security*, vol. 2012, no. 10, pp. 15-17.
- Cluley, G. (2011), (2011), June 1-last update, *Rihanna and Hayden Panettiere sex video spreads Mac malware on Facebook* [Homepage of Sophos], [Online]. Available: <http://nakedsecurity.sophos.com/2011/06/01/rihanna-hayden-panettiere-lesbian-sex-video-mac-malware-facebook/> [2013, 01/17].
- Corrons, L. (2012), *Katy Perry and Russell Brand baits to spread a new Facebook worm* [Homepage of Pandasecurity], [Online]. Available: <http://pandalabs.pandasecurity.com/katy-perry-and-russell-brand-baits-to-spread-a-new-facebook-worm/> [2013, 01/27].
- Faghani, M.R. & Saidi, H. (2009), "Malware propagation in online social networks", *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on IEEE*, pp. 8.
- Galperin, E. & Marquis-Boire, M. (2012), 2012, March 29-last update, *Syrian Activists Targeted With Facebook Phishing Attack* [Homepage of Electronic Frontier Foundation], [Online]. Available: <https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack> [2013, 01/27].
- Grandjean, E. (2008), "A prime target for social engineering malware", *Mcafee security journal*'Debuts, , pp. 16.
- Hadnagy, C. (2010), *Social Engineering: The Art of Human Hacking*, 1st edn, Wiley.
- Kritzinger, E. & von Solms, S.H. (2010), "Cyber security for home users: A new way of protection through awareness enforcement", *Computers & Security*, vol. 29, no. 8, pp. 840-847.
- Kuo, C., Schneider, F., Jackson, C., Mountain, D. & Winograd, T. (2005), "Google Safe Browsing. Project at Google", *Inc., June–August*, .
- Labuschagne, W.A., Eloff, M.M. & Veerasamy, N. (2012), "The dark side of Web 2.0", *IFIP Advances in Information and Communication Technology*, vol. 386/2012, no. ICT Critical Infrastructure and Society, pp. 237-249.
- Larson, D. (2012), *Infographic: Spring 2012 Social Media User Statistics* [Homepage of Tweetmaster.com], [Online]. Available: <http://blog.tweetsmarter.com/social-media/spring-2012-social-media-user-statistics/> [2013, 01/25].
- McGarry, C. (2012), *Nielsen survey: Social media sucking up most of our time* [Homepage of PCWorld.com], [Online]. Available: <http://www.pcworld.com/article/2019194/nielsen-survey-social-media-sucking-up-most-of-our-time.html> [2013, 01/25].



McMillan, R. (2011), *Facebook video scam puts malware on Mac and Windows* [Homepage of computerworld.com], [Online]. Available: [http://www.computerworld.com/s/article/9217229/Facebook\\_video\\_scam\\_puts\\_malware\\_on\\_Mac\\_and\\_Windows](http://www.computerworld.com/s/article/9217229/Facebook_video_scam_puts_malware_on_Mac_and_Windows) [2013, 01/27].

Protalinski, E. (2012), *Facebook to expose hackers behind Koobface worm* [Homepage of ZDNet], [Online]. Available: <http://www.zdnet.com/blog/facebook/facebook-to-expose-hackers-behind-koobface-worm/7462> [2012, 09/19].

Provos, N., McNamee, D., Mavrommatis, P., Wang, K. & Modadugu, N. (2007), "The ghost in the browser analysis of web-based malware", *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets* USENIX Association, Berkeley, CA, USA, pp. 4.

Runald, P. (2010), *Most Hilarious Video attack on Facebook* [Homepage of Websense], [Online]. Available: <http://community.websense.com/blogs/securitylabs/archive/2010/05/28/most-hilarious-video-attack-on-facebook.aspx> [2013, 01/27].

Smith, C. (2011), *Facebook Malware Attack: Fake Strauss-Kahn Video Infects Mac And PC Users (UPDATE)* [Homepage of The Huffington Post], [Online]. Available: [http://www.huffingtonpost.com/2011/06/01/facebook-malware-strauss-kahn-video\\_n\\_869576.html](http://www.huffingtonpost.com/2011/06/01/facebook-malware-strauss-kahn-video_n_869576.html) [2013, 01/27].

Villeneuve, N., Deibert, R. & Rohozinski, R. (2010), *Koobface: Inside a crimeware network*, Munk School of Global Affairs.

Wondracek, G., Holz, T., Platzer, C., Kirda, E. & Kruegel, C. (2010), "Is the Internet for porn? An insight into the online adult industry", *Proceedings (online) of the 9th Workshop on Economics of Information Security*, Cambridge, MA.

Yee, K.P., Swearingen, K., Li, K. & Hearst, M. (2003), "Faceted metadata for image search and browsing", *Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM, , pp. 401.

## **Towards an automated security awareness system in a virtualized environment**

William Aubrey Labuschagne <sup>1</sup>, Mariki Eloff <sup>2</sup>

<sup>1</sup> Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa

<sup>2</sup> School of Computing, University of South Africa, Pretoria, South Africa

wlabuschagne@csir.co.za

Eloffmm@unisa.ac.za

**Abstract:** A majority of African Internet users do not have access to the Internet. The lack of infrastructure in rural areas affects Internet usage. Since costs are high and the bandwidth low, these factors encourage users to access the Internet using shared resources. This is an efficient solution to access the Internet. However users might not be aware of the security threats that exist on using shared resources. Many companies provide security solutions to automatically protect resources on the network and security awareness training to users. This ensures that users are aware of the security threats and provide methods to mitigate them. These measures are useful in a corporate environment where funds exist to enable these security solutions. Public platforms, for example Internet Cafes and schools, allows multiple users to access the Internet using shared resources. This implies that multiple people will use the same computer to perform required tasks. Numerous security threats exist within the Internet sphere that could affect users utilizing shared resources these include but are not limited to viruses, keyloggers and phishing attacks. This shared environment could provide a platform that promotes the spread of virus infections. Users using these platforms should be made aware of these threats and monitor the effectiveness of the security awareness campaign. This paper proposes a system used to address these issues from a single platform. The Shared Public Security Awareness (SPSA) system is an automated virtualized system used to determine the current security awareness levels of users on a shared platform accessing the Internet. The system uses virtual machines to provide users with access to the Internet, assess the security awareness levels of the users, determines if any web browser components were infected by web based malware during browsing sessions, provides users with access to security related material affecting the users and provide reports on online behaviour. This paper evaluates the proposed SPSA system as a mechanism to conduct a security awareness campaign in a shared resource environment while providing a capability to analyze the online behaviour of users that affects the security of this environment.

**Keyword:** Internet cafes, security awareness, security training, virtualized environments, cyber literacy, Internet

### **1. Introduction**

The Internet provides a vast range of information resources and services which form part of everyday life. Usages include but are not limited to searching for information, conducting business, paying bills and the purchase of goods. Moreover the development of human capital has been identified as an important economical performance indicator in rural areas (Agarwal, Rahman & Errington 2009). This can be attained with access to knowledge available on the Internet. However the high adoption and use of the Internet by citizens introduced an opportunity for cyber criminals to utilize this platform to coordinate cyber attacks with the intention to cause damage. Kim identified a comprehensive list which includes loss of money, defamation, invasion of privacy, physical harm, loss of time and psychological damage (Kim et al. 2011). Most companies provide security measures against these attacks for their employees. In most instances employees require to attend security awareness training programs to equip them with strategies on how to mitigate these cyber attacks when encountered. Furthermore the network infrastructure is secured with expensive security solutions. Therefore, people working at companies are best equipped against cyber attacks. Users in rural areas are in a disadvantages position. In most instances these users do not have ownership of resources to access the Internet. The cost of access to the Internet and equipment inhibits ownership of resources like computers. The need to access the Internet was addressed with entrepreneurial initiatives which provide access to the Internet with the use of shared resources. This implies multiple users using the same computer to access the Internet. An example of this implementation are schools and Internet cafes. However, users sharing the same resources could assist in the spread of malware infections. In the event of discovering a malware infection at these establishments, the services provided need to be suspended which has an effect on revenue for the owners. Another issue which could be encountered at these establishments is security literacy.

Most of these users are not aware of the cyber threats that are devised and deployed by criminals. Security awareness programs are used to educate the users and provide them with measures to identify and mitigate the threats encountered. Grobler studied the cyber awareness initiatives in South Africa (Grobler et al. 2011). She reported on initiatives by the Council for Scientific and Industrial Research (CSIR), the University of

Pretoria (UP), the University of Fort Hare (UFH) and Nelson Mandela Metropolitan University (NMMU). The CSIR collaborated with the University of Venda to raise security awareness in the rural areas by developing content which addresses cyber security topics and training community members which then in turn will train the community. The UP project, PumaScope, equips students with the required security knowledge to educate scholars at identified schools. UFH tested the proficiency levels of the user in a particular area. NMMU addresses educating users through the use of games and e-learning platforms to provide access to security awareness content for a wider audience. A need has been identified to provide an automated platform which incorporates the core ideas of the mentioned initiatives a platform that could be used to determine the proficiency levels of the users and provide access to resources to improve security awareness in rural areas.

This paper looks at the design of an automated tool, Shared Public Security Awareness (SPSA) system, which promotes security awareness in rural areas where the community uses shared computer resources to access the Internet. These resources can be located at schools or Internet café where access to the Internet is provided through the use of shared computers. Establishments would be used throughout the paper that references the communal area where the shared computer resources are located. The deployment of the SPSA system addresses three primary functions: The first function is to provide the capability to conduct a security awareness program which consist of assessing the literacy of the users and deliver the security awareness topics to the users. The second function analyzes the online behaviour of users and the collection of malware which would assist in developing strategies which addresses the security threats encountered at these establishments. The third function provides a turnkey solution which automates the functionality of the SPSA system with limited intervention from personal to administrate the system.

The rest of the paper is organized as follows: section 2 summarizes research related to the component identification of the SPSA system. The main contribution: the design of the SPSA system is outlined in section 3. Conclusions and future work are discussed in section 4.

## **2. Related Research and Underlying Concepts**

The SPSA virtualized and collection system requirements are discussed in this section. These establishments provide resources which enables user's access to the Internet through the use of web browsers. Cyber attackers have adopted attacking strategies which include automated exploitation of computer systems without the intervention of the user. The resources used by these establishments must be protected against possible attacks originating from the Internet. Also a mechanism is required to identify the threat and evaluate the actions performed by users which initiated these attacks. The system should exhibit the following capabilities:

- 1) A robust and automated architecture which ensures availability and configurability of the system. This is achieved with the implementation of virtualization and customization of existing systems (See Section 2.1).
- 2) The identification of threats originated from users visiting malicious web sites, accomplished with the collection and analysis of data generated during browsing sessions (Section 2.2).

### **2.1 Virtualization, automation and customization**

The SPSA system underlying architecture consists of virtual machines. Bell defines a virtual machine as software that functions as a computer without physically being a computer (Bell, Lintumaa 2011). The use of virtual machines provides numerous of advantages.

The implementation of virtualized environments is cost effective. England proposed a model for deploying virtual machines as a securing mechanism for the enterprise desktop (England, Manferdelli 2006). Some organizations require users to conduct classified work. In these organizations the users will be provided with two physical computers: one to conduct normal duties and the other for classified duties. This is not cost effective. The use of virtual machines would allow both functionalities to be conducted within a virtualized environment and provide the required security measures.

Virtual machines can be controlled programmatically with the use of scripting language which automates the process of operations which include start-up and shutdown. Light proposes the use of scripts to control virtual machines within an automated sandbox (Ligh et al. 2010). He also described the malware analysis cycle with the use of virtualization which is supported by Harlan (Harlan 2005). The cycle described by Light is adapted for the SPSA system. A baseline virtual machine is created. A copy is made of the baseline virtual machine and then loaded daily for usage at these establishments. This will ensure that uninfected virtual machines are deployed for use every day. It also provides the opportunity to examine the virtual machines for possible infections; this is achieved by storing the virtual machine used during the day.

The added benefit of virtual machines is the efficiency of restoring to a state which users can use to access the Internet after malware infections. An environment which uses physical machines requires reinstalling the operating system after a malware infection. During this period the establishment cannot conduct business. The use of virtual machines minimizes the period of inactivity. Gold reported in 2007 of cyber attackers targeting virtualization (Steve 2007). Some malware is virtual machine aware which implies that the malware would not execute in the virtual machine environment (Zhu, Chin 2007). The malware writers added this feature to protect the malware against virtualised environments used by malware analysts. This could be beneficial to the establishments and reduce the infection rate due to the inactivity of the malware.

Users at establishments require access to the Internet. A customizable user management system would be required to control the sequence users follow to access the Internet and expose features of the SPSA system to the users. These features include the completion of a questionnaire and coverage and comprehension of the security awareness topics. The continuous exposure to security related content contributes the success of a security awareness program (Kruger, Kearney 2006). The SPSA system is designed to present security awareness content to the user before accessing the Internet thus reminding the user of safe practises against cyber attacks. Easyhotspot is an alternative solution for hotspot billing system released under the GNU general public license which implies that the software could be modified with the needed requirements of the SPSA system (The EasyHotspot team 2007). Easyhotspot consists of a user management system which allows users to access the Internet through the portal (See Figure 1). Modifications to the portal would presents users with access to the security awareness content or the questionnaire.



**Figure 1: EasyHotspot Management System**

## 2.2 Threat collection and analysis

Abraham summarised an overview of social engineering malware which entices users to perform detrimental actions which could infect the computer system (Abraham, Chengalur-Smith 2010). The malware utilizes numerous avenues which include websites, social software and email for infection. Web browsers are used to access these avenues on the Internet. The inspection of the web sites visited is crucial in the identification of threats and determining the effectiveness of the security awareness program. Polychronakis proposed the design of a URL collection system used in exploring the life cycle of web based malware (Polychronakis, Mavrommatis & Provos 2008). The system analyzed the web pages for malicious content; this was achieved by visiting the URL and monitoring the system for new processes, file system changes and registry modifications. Provos also proposed a similar approach which consisted of identification of URL's, in-depth verification of maliciousness and aggregation of malicious URL's into site level ratings (Provos et al. 2007). These approaches are risky; a controlled approach is required by collecting the content from the URL and testing the content for maliciousness. Collection of the content from the web sites could be achieved with a web crawler. Mohr discussed Heritrix which is an open source extensible, web scale, archival-quality web crawler (Mohr et al. 2004). Ikinici demonstrated the effectiveness of Heritrix as part of the MonkeySpider

system used in the detection of malicious websites (Ikinci, Holz & Freiling 2008). The SPSA system follows a similar approach as demonstrated in the MonkeySpider system which includes the use of antivirus software in the identification of malicious content. These components discussed provide an automated and virtualized platform for the SPSA system.

The following section discusses the technical implementation of the components.

### 3. Shared Public Security Awareness (SPSA) System Architecture

The SPSA system consists of subsystems which as whole provide a virtualized automated platform to access the Internet, collect Internet behavioural data and delivery of a security awareness program at these establishments. These subsystems can operate independently of each other and thus are discussed separately. The automated virtualized environment is discussed in Section 3.1 and 3.2, followed by Section 3.3. and 3.4 which addresses the collection of data generated during browsing sessions and concluding with the elaboration of the security awareness program delivery mechanism in Section 3.5 and 3.6.

#### 3.1 Internet Access System

The Internet Access System is a modified user management system which based on configuration will direct users first to complete the security awareness questionnaire or direct users to the security awareness content before allowing access to the Internet (See Figure 2). The selection policy determines which functionality the user will interact with. The questionnaire functionality is used to assess the security knowledge of the user while the content functionality provides the user with an opportunity to learn about security related topics.

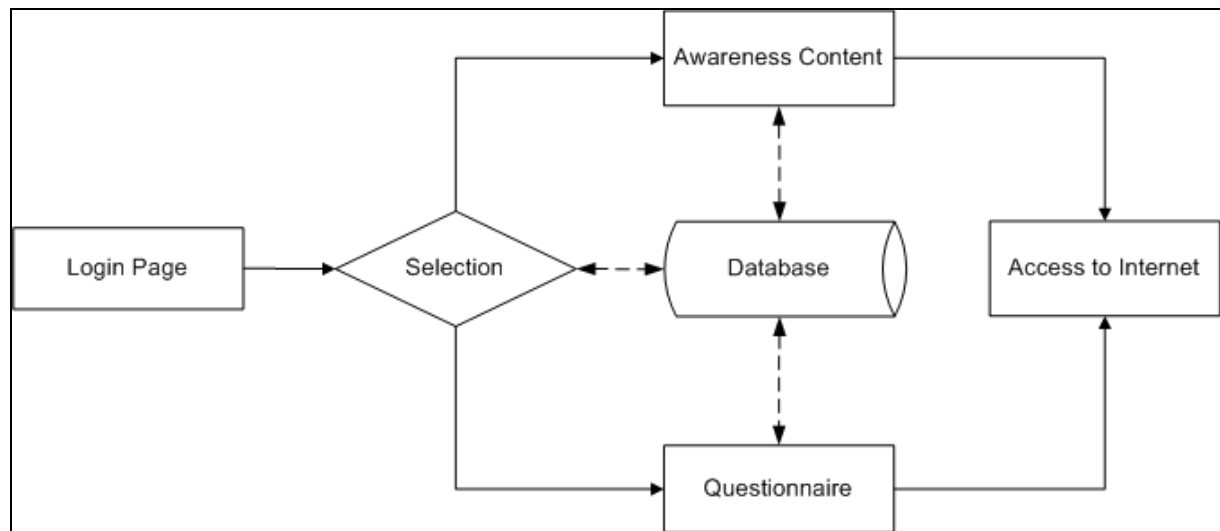
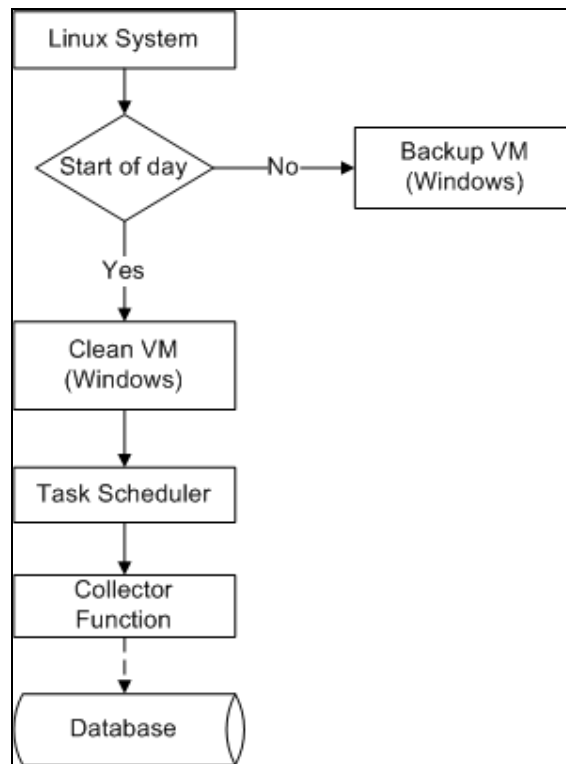


Figure 2: Internet Access System

#### 3.2 Virtual Machine Manager

The Virtual Machine (VM) Manager automates the operations of the SPSA system (See Figure 3). At the start of each day the VM manager loads a “clean” virtual machine for usage. A “clean” virtual machine represents a baseline installation of the operating system which has not been used by the users of these establishments. All components required to access the Internet are installed and configured. During the setup phase all software is tested for viruses and only reputable websites are visited to download software or update software. The task scheduler will initiate predefined scripts which will activate the URL collection system to capture HTTP packet information into a file. Users will arrive at the workstations and start browsing websites. At the end of the day the task scheduler will initiate a script which will extract the data out of the file created and store the data in a database. The VM manager will shutdown the virtual machine which was used during the day, creates a backup of the virtual machine and assigns a date label to the virtual machine should forensics or malware analysis be required on the virtual machine.



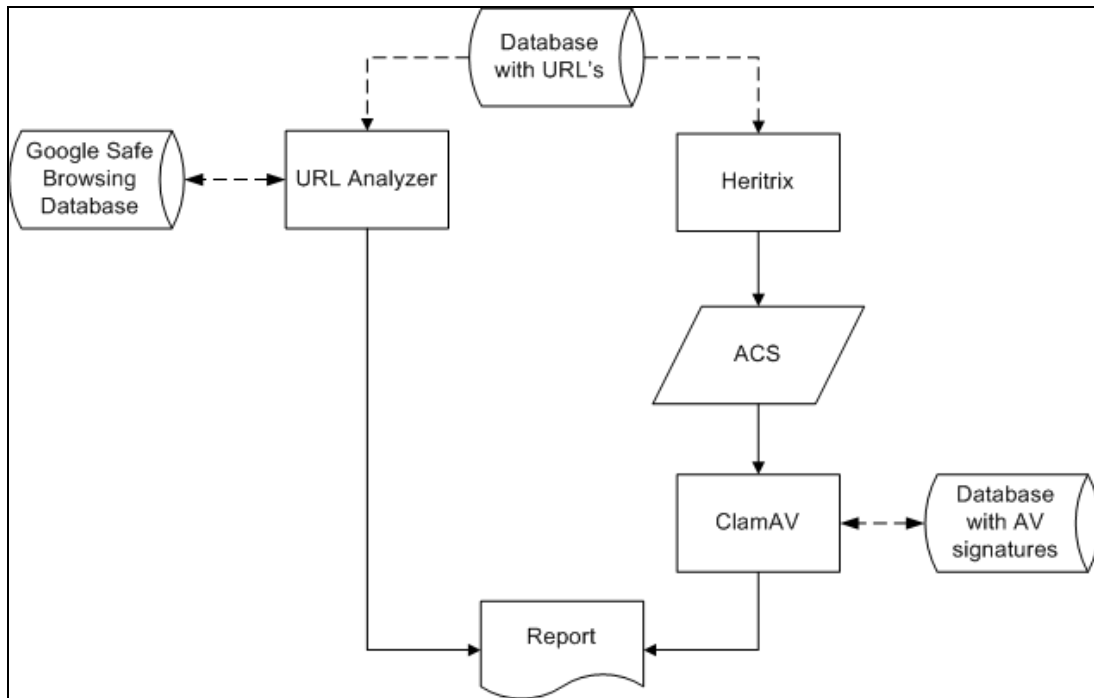
**Figure 3: Daily Virtual Machine Operations**

### 3.3 URL Collection System

The URL collection system is used in the collection of the web page address visited by the user and these include the web pages that are visited without the prior knowledge of the user. The URL collection is initialized during the start sequence of the user's virtual machine. TShark is a network protocol analyzer which provides the capability to capture packet data from a live network. Studies conducted by (Nascimento, Correia 2011) and (En-Najjary, Urvoy-Keller 2010) used TShark for the collection of specified network traffic. During the operation of the SPSA system a filter will be used to specify the required data to capture. Only outgoing HTTP traffic data is required which saves disk usage. The request line in the HTTP data packet contains the required data. The URL information is important to the work described here. According to (Forouzan 2003), "The URL is a standard for specifying any kind of information on the Internet. The URL defines four things: method, host computer, port, and the path." He states that host and path provide information on where the information is located. The URL provides a route to the content that was accessed by the user. TShark filter is configured only to collect the request line information encapsulated in the Hypertext Transfer Protocol (HTTP) header. An output file containing the captured data will be created when the time expires. This will contain the address of the webpage the user visited. Storage of the data is required and this is achieved by the URL transporter system which will analyze and extract the data from output file created by TShark. The URL transporter system is an application which will be executed at predetermined times during the day to poll a specified directory and extract the data from all the files within the directory and transport it to the external storage components for example a database server.

### 3.4 URL Inspector

The URL Inspector component is designed to examine the URL's visited by the user. It consists of two components namely the URL Analyzer and the Malware Collection and Classification (MCC) system (See Figure 4). The URL Analyzer will examine each collected URL in the database against the Google Safe Browsing database, a service provided by Google, which enables applications to examine the location of the website against known phishing and malware websites (Google Code Lab 2008). This information is captured in a report. The MCC system also uses the URL captured in the database. The system consists of an Internet crawler called Heritrix which will be used to download the content of the URL and then use an anti-virus (AV) application called ClamAV to determine if the content is malicious. The list of malware found will be captured in a report. The report could assist in the identification of threats specific to these establishments and be used as a measure to determine the effectiveness of security awareness programs.



**Figure 4: URLInspector**

The data gathered about the browsing behaviour which include the destination address and the content of the web pages visited will be useful to determine the effectiveness of security awareness campaign by investigating the behavioural changes of the Internet users at these establishments

### 3.5 Awareness Collection System

The security awareness levels of the users will be determined by completing a questionnaire. The users visiting these establishments are required to login. Thereafter the users will be presented with a set of questions which assesses the knowledge in security awareness related topics. Wilson reported on the best practises in the development of a security awareness program (Wilson, Hash 2003). One of the sections in the report discussed a comprehensive list of awareness topics some of these include but is not limited to:

- Password usage and management
- Spam
- Social Engineering
- Web usage
- Shoulder surfing
- Desktop security
- Unknown e-mail/attachments
- Incident response – contact whom? “What do I do?”

The Awareness Collection System was developed with requirements identified for the design of a security awareness game (See Figure 5). Game play encourages learning and with the use of game play components users are enticed to return to continue with the game. Using these principles would extend the contact time between the SPSA system and the user. Labuschagne recommended the use of Appointment, Influence and Status, and Progression dynamics (Labuschagne et al. 2011a). These dynamics are demonstrated visually with the use of badges. A badge is a visual indicator of an achievement. The appointment dynamic is represented with an image and is calculated with the consecutive logins over a period of three days. The user has to ensure that they continuing using the system after the badge have been obtained. The badge would be revoked should the user miss one day from using the system. The badge will be assigned again to the user after three consecutive day usage of the system. The status badge is provided when a user answers five questions correctly. The badge will be revoked in the event of an incorrect answer. Therefore the user is encouraged to provide the correct answers. The progression

dynamic is represented with the progress bar which provides the user with a visual indicator on progress. The user is presented with randomized multiple choice questions. Labuschagne also identified security awareness topics which are applicable to establishments which allow resources to be shared amongst users accessing the Internet (Labuschagne et al. 2011b). These topics are more specific to the environment and include social media security awareness topics which is lacking in the work conducted by Wilson (Wilson, Hash 2003). The questions categories include but are not limited to the following:

- Spam
- Cyber bullying
- Malware
- Social Engineering
- Social Networking Sites
- Phishing

The screenshot displays a user interface for a security awareness questionnaire. At the top, there are sections for 'You' (with a profile picture) and 'Badges' (with a red cube icon). Below this is a 'Progress' section with a horizontal bar indicating 16% completion. The main question reads: 'On the Facebook page, you notice under the links to the "Info" and "Photo" sections are links to three offers. What type of attack could this be?'. The question is illustrated with a screenshot of a Facebook page for 'I Love Michael Jackson' featuring a 'Get a FREE iPad 2' offer with a 'Click Here' button. Below the question, there are five radio button options: 'Phishing', 'Malware', 'Social Engineering', 'Scam', and 'Cyber bully'. At the bottom left, there is an 'Answer' button.

**Figure 5: Screenshot of Security Awareness Questionnaire**

A report will be generated upon the completion of the questionnaire. The report indicates areas of weakness for the user and provides the user access to resources which addresses the areas of concern. A comprehensive report could assist in the identification of security awareness topics specific to the establishment. These results could also be incorporated in to the E-Awareness Model (E-AM) proposed by Kritzinger and Von Solms. This model would not allow home users to access the Internet if their security awareness levels are not satisfactory. Also the users are required to complete remedial work to address the shortcomings before access to the Internet is granted (Kritzinger, von Solms 2010). The SPSA system is designed to determine the security awareness levels and provide users to opportunity to improve their security knowledge with topics specific to users at these establishments.



### 3.6 Awareness Content System

The Awareness Content System makes use of a content management system (CMS) to deliver the material to the user. The CMS used for the study purpose is called Moodle. It is a software package for producing Internet-based courses and web sites (Dougiamas 1999). Some typical features of Moodle are assignment submission, discussion forum, files download, grading, instant messages, online calendar, online news and announcement, online quiz and a wiki. These features provide a platform that integrates into the requirements of the SPSA system in the delivery of security awareness content to the users and provide a mechanism for assessment. The CMS stores that material of the identified security awareness topics which the user can easily access. One of the topics addresses the dangers of short URL's which could be encountered on social media platforms (See Figure 6). The user is provided with background information on the threat and suggests actions to perform once the threat is encountered. The CMS also provides functionality to assess the user's knowledge on the topic that was accessed by the user. The material content is collected from different sources which include vendor specific security best practises provided to the community. For instance, McCarthy composed a guide to Facebook security which addresses safety topics relating to the social networking platform (McCarthy, Watson & Weldon-Siviy 2011). One of the topics in this guide provides readers the necessary steps required to protect their Facebook accounts. The material for the SPSA system is updated once new information has become available. The material on the SPSA needs to current to address the latest threats identified by security vendors. This is possible by following information security threat trends that affects the categories identified for the establishments.

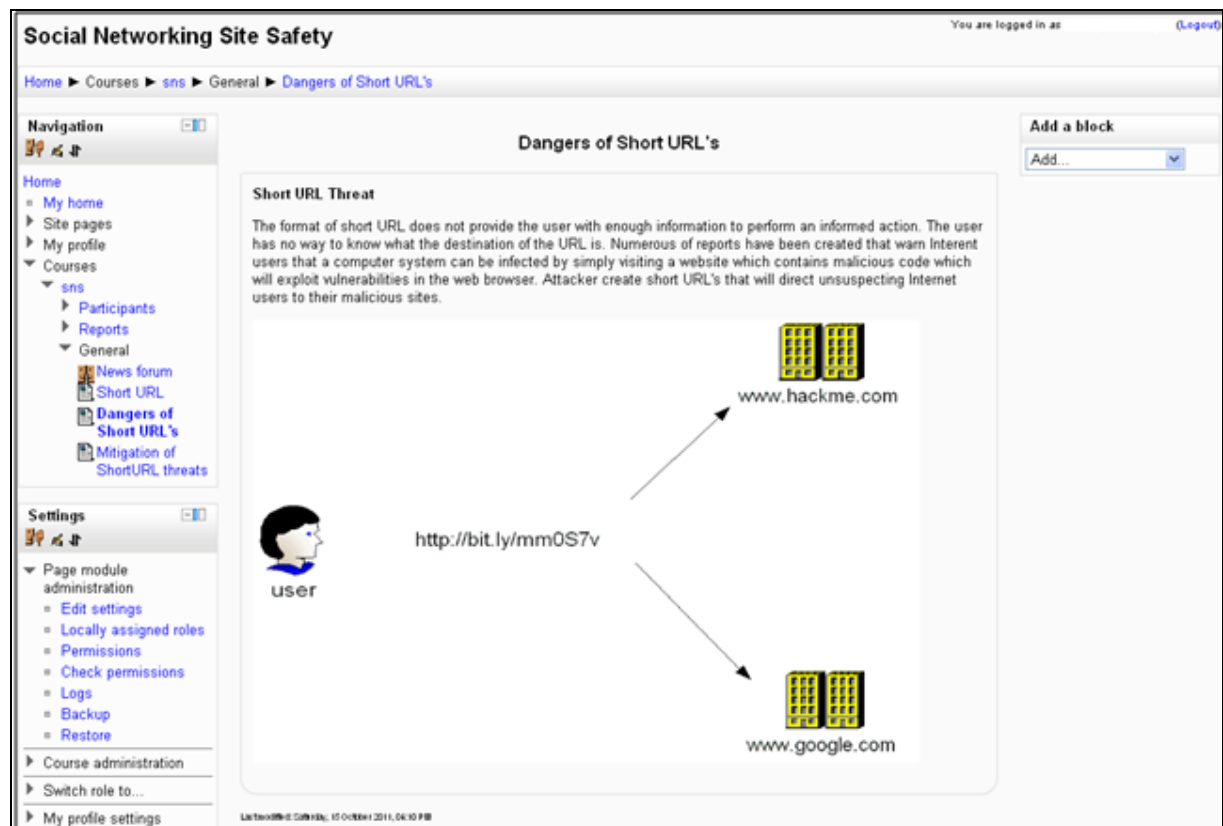


Figure 6: Awareness Content System

### 4. Conclusion

This paper describes the design of an automated and virtualized platform used to promote security awareness in rural areas where the community access the Internet through shared resources. The SPSA system is a collection of components identified in the body of knowledge which provides a singular tool to measure the proficiency of the community and promotes security awareness. The SPSA system resolves the problem of associated with conducting security awareness programs in rural areas; these include but is not limited to travelling to the destination, establishing trust with the community and the frequency of exposing the users at these establishments to security related content. It provides an automated and virtualized infrastructure which improves the availability of resources to access the Internet, collects data about the browsing behaviour of the users, the identification and classification of threats encountered by the users, and

conducts a security awareness program. The SPSA system does however have limitations. Currently the SPSA system consists of two subsystems: The automated virtualized platform which delivers the security awareness program and a separate platform which is designed for the evaluation of content visited by the users during the browsing session. The process to transfer the data collected by the automated virtualized platform is not automated. The majority of these establishments do not have the infrastructure to provide enough bandwidth to harvest all the content from the web pages as this process requires the research team to collect the data from the establishments and complete the process at another location which provides high bandwidth infrastructure. Furthermore the identification of malicious sites and software is limited to the signatures identified by security vendors. The SPSA system does not provide a component to automatically update the security awareness content.

Future research will include an additional component to determine if the virtual machine used by the user resembles malware infection behaviour. This would improve the accuracy of malware infection identification. In addition, the SPSA system requires a mechanism to assess the factors affecting the behavioural change of the users at these establishments. This is required to evaluate the effectiveness of the SPSA system. The evaluation of the effectiveness of the SPSA system would be determined with the deployment of the system in identified rural areas.

## References

- Abraham, S. & Chengalur-Smith, I. 2010, "An overview of social engineering malware: Trends, tactics, and implications", *Technology in Society*, vol. 32, no. 3, pp. 183-196.
- Agarwal, S., Rahman, S. & Errington, A. 2009, "Measuring the determinants of relative economic performance of rural areas", *Journal of Rural Studies*, vol. 25, no. 3, pp. 309-321.
- Bell, M. & Lintumaa, K. 2011, *Virtual Machines: Added planning to the forensic acquisition process.*, InSecure.
- Dougiamas, M. 1999, *Modular Object-Oriented Dynamic Learning Environment*, 2.1.2 edn, Moodle Pty Ltd.
- England, P. & Manfredelli, J. 2006, "Virtual machines for enterprise desktop security", *Information Security Technical Report*, vol. 11, no. 4, pp. 193-202.
- En-Najjary, T. & Urvoy-Keller, G. 2010, "A first look at traffic classification in enterprise networks", *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference* ACM, , pp. 764.
- Forouzan, B.A. 2003, "Hypertext Transfer Protocol" in *TCP/IP Protocol Suite*, 2nd edn, McGrawHill, , pp. 649-663.
- Google Code Lab 2008, *Google Safe Browsing*. [online], <http://code.google.com/apis/safebrowsing/>
- Grobler, M., Flowerday, S., Von Solms, R. & Venter, V. 2011, "Cyber Awareness Initiatives in South Africa: A National Perspective", *Southern African Cyber Security Awareness Workshop* Defence, Peace, Safety and Security (CSIR), South Africa, 12 May 2011, pp. 32.
- Harlan, C. 2005, "Malware analysis for windows administrators", *Digital Investigation*, vol. 2, no. 1, pp. 19-22.
- Ikinci, A., Holz, T. & Freiling, F. 2008, "Monkey-spider: Detecting malicious websites with low-interaction honeyclients", *Proceedings of Sicherheit, Schutz und Zuverlässigkeit*, .
- Kim, W., Jeong, O., Kim, C. & So, J. 2011, "The dark side of the Internet: Attacks, costs and responses", *Information Systems*, vol. 36, no. 3, pp. 675-705.
- Kritzinger, E. & von Solms, S.H. 2010, "Cyber security for home users: A new way of protection through awareness enforcement", *Computers & Security*, vol. 29, no. 8, pp. 840-847.
- Kruger, H.A. & Kearney, W.D. 2006, "A prototype for assessing information security awareness", *Computers & Security*, vol. 25, no. 4, pp. 289-296.
- Labuschagne, W.A., Burke, I., Veerasmay, N. & Eloff, M.M. 2011a, "Design of cyber security awareness game utilizing a social media framework.", *Information Security South Africa* South Africa, 15 May 2011.
- Labuschagne, W.A., Eloff, M.M., Veerasmay, N., Leenen, L. & Mujinga, M. 2011b, "Design of a Cyber Security Awareness Campaign for Internet Cafe Users in Rural Areas", *Southern African Cyber Security Awareness Workshop* Defence, Peace, Safety and Security (CSIR), South Africa, 12 May 2011, pp. 42.
- Ligh, M.H., Adair, S., Hartstein, B. & Richard, M. 2010, *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, 1st edn, Wiley.

- McCarthy, L., Watson, K. & Weldon-Siviy, D. 2011, *A Guide to Facebook Security For Young Adults, Parents, and Educators*, Facebook.
- Mohr, G., Kimpton, M., Stack, M. & Ranitovic, I. 2004, "Introduction to Heritrix an archival quality web crawler", *Proceedings of the 4th International Web Archiving Workshop (IWAW'04)*, sep.
- Nascimento, G. & Correia, M. 2011, "Anomaly-based Intrusion Detection in Software as a Service", .
- Polychronakis, M., Mavrommatis, P. & Provos, N. 2008, "Ghost turns zombie: exploring the life cycle of web-based malware", *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*USENIX Association, Berkeley, CA, USA, pp. 11:1.
- Provos, N., McNamee, D., Mavrommatis, P., Wang, K. & Modadugu, N. 2007, "The ghost in the browser analysis of web-based malware", *Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*USENIX Association, Berkeley, CA, USA, pp. 4.
- Steve, G. 2007, "Time to face virtualized realities", *Infosecurity*, vol. 4, no. 4, pp. 35-38.
- The EasyHotspot team 2007, *EasyHotspot.*, [online], <http://easyhotspot.inov.asia/>
- Wilson, M. & Hash, J. 2003, *Building an Information Technology Security Awareness and Training Program*, National Institute of Standards and Technology, Gaithersburg.
- Zhu, D. & Chin, E. 2007, "Detection of VM-Aware Malware", University of Berkeley, [online], [http://radlab.cs.berkeley.edu/w/upload/3/3d/Detecting\\_VM\\_Aware\\_Malware.pdf](http://radlab.cs.berkeley.edu/w/upload/3/3d/Detecting_VM_Aware_Malware.pdf)

# The dark side of Web 2.0

WA Labuschagne<sup>1,2</sup>, MM Eloff<sup>2</sup>, N Veerasamy<sup>1</sup>

<sup>1</sup> CSIR, Pretoria, South Africa

{wlabuschagne, nveerasamy}@csir.co.za

<sup>2</sup>School of Computing, Unisa, South Africa

Eloffmm@unisa.ac.za

**Abstract.** Social networking sites have increased in popularity and are utilized for many purposes which include connecting with other people, sharing information and creating content. Many people on social networking sites use these platforms to express opinions relating to current affairs within society. People do not realize the value of their data divulged on these platforms and the tactics implemented by social engineers to harvest the seemingly worthless data. An attack vector is created when a user can be profiled using responses from one of these platforms and the data combined with leaked information from another platform. This paper discusses methods for how this data, with no significant value to the users, can become a commodity to social engineers. This paper addresses what information can be deducted from responses on social news sites, as well as investigating how this information can be useful to social engineers.

**Keywords:** Digital Footprint, Facebook, Information Gathering, Internet, LIWC, Social Engineering, Social Media, Profiling, Web 2.0

## 1 Introduction

Social engineering is the process of manipulating people into performing actions or divulging confidential information which they would not have done under ordinary circumstances. This statement is supported by Mann, author of “Hacking the Human,” who defines social engineering as means to manipulate people by deception resulting in them giving out information or performing an action [1].

Numerous studies have indicated that the human element is the weakest link in information security, and cyber criminals have adapted attacks to include this human element [2][3]. Most of the security tools deployed to protect assets within the corporate environment have made it more challenging for attackers to gain access to the corporate network infrastructure. Cyber criminals have adapted to these changes and are adopting social engineering as part of their cyber attacks. The success of social engineering attacks relies on the accuracy of the data collected allowing the attacker to profile the target.

Profiling allows the attackers to predict the behavior of the victims and this is made possible by recording and analyzing the psychological and behavioral characteristics of the target [4]. A social engineer prefers anonymity which results in the search for a

platform which stores valuable and collectable data while protecting the attacker's anonymity. Anonymity defends the attackers from any form of network surveillance which could be used to track the location and identity of the perpetrator. Web 2.0 provides such a platform.

In this paper we investigate how cyber criminals could aggregate the posts and comments on a web platform for malicious intent as part of information gathering used during a social engineering attack. In our investigation we test our approach with a proof-of-concept to determine the adverse effects of participation on Web 2.0 platforms like online news websites and social networking sites. Online news websites allow users to express their opinions on news articles, through posts and comments. In addition, users are permitted to participate on news websites using other social networking sites' login credentials which could be used in harvesting additional data about the user.

The remainder of this paper is structured as follows: Section 2 summarizes other research related to profiling and underlying concepts. Our contribution to the research field is discussed in Section 3. Users on social networking sites are not aware of the value of the data they divulge unknowingly. The work in this paper demonstrates how the user's digital footprint could be used for nefarious purposes. User awareness of techniques used by cyber criminals is essential in the protection against threats from cyber space. The findings add to the body of knowledge in the security awareness domain. The implementation follows in Section 4. The findings are discussed in Section 5 and in Section 6 we discuss an example of how the data could be used. Future work is explained in Section 7. We conclude the paper in Section 8.

## **2 Related Research and Underlying Concepts**

This section describes how social engineers could use the digital environment to harvest valuable data as part of an attack. Thereafter a description is given on how the textual data was analyzed before concluding with the potentially nefarious uses of social networking sites by terrorists and infiltration of critical infrastructures using social engineering.

### **2.1 Digital Environment**

Social engineers require information to initiate a social engineering attack. Social networking sites provide a digital platform to harvest and collect data. Social media sites like news websites allow users to post opinions on published articles and comment on posts created by other users. Evans, Gosling and Carroll suggested an individual's personality could be effectively communicated to other users using social networking sites [5]. One of their findings concluded that men are more likely to disclose political views than women. Social engineers could use this information to either build trust with the target or as an emotional trigger. The use of function words within sentences offers insight into the honesty, stability, and self-image of the person

[6]. Furthermore the language use in self-narratives could be used to determine personalities [7]. An investigation by Ryan and Xenos summarized the Big Five and the usage of Facebook [8]. The Big Five are defined as five broad domains or traits of personality used to describe the human personality. The Big Five traits are openness, conscientiousness, extraversion, agreeableness, and neuroticism. For example, neurotic people are easily stressed and upset [9]. This trait can be easily exploited by social engineers.

This iterates the point on gathering reliable and valid information about the target improves the success rate of a social engineering attack. Similarly, the Department of Homeland Security in the United States of America investigated the possibility to predict when terrorist might launch an attack. The predictions were deduced from 320 translations of Arabic of documents released by the terror groups: al-Qaeda, al Qa'ida, Hizb ut-Tahrir, and the Movement for Islamic Reform in Arabia (MIRA) [10].

Social media have been identified as one of the sources from which data can be collected. The following section describes the application used to analyze the data collected.

## 2.2 Linguistic Inquiry and Word Count

This section provides a brief overview of linguistic analysis and how writing styles can be analyzed. It also describes how terrorists could use social networking sites and how critical infrastructures could be infiltrated using social engineering techniques.

Linguistic Inquiry and Word Count (LIWC) is a probabilistic text analysis program that counts words in psychological meaningful categories. These categories include but are not limited to positive emotions, negative emotions, social words, anger [11]. Consequently LIWC could be used to identify social relationships, emotions and thinking styles from textual data representing human communication. The clarification is made possible by the design of LIWC which consists of two components: the processing components and the dictionaries. The processing component opens a file containing the text and compares each word within the file with the dictionary file subsequently classifying each word to a corresponding category. Next LIWC calculates the percentage for each category. For example consider the following sentence: "*Today is a beautiful day*". LIWC would first take the word "*Today*" and determines if it belongs to one or more categories. The program would increment each of the categories the word is associated with and select the next word until all the words in the file are analyzed. If a word belongs to more than one category then all the relevant categories will be incremented. Consequently LIWC would calculate the percentages for each category for example positive (5%) which implies that the text contains 5% of positive words. The percentage is calculated by dividing the sum of a category by the word count resulting in the following output: function (40%), article (20%), verb (20%), auxiliary verb (20%), present tense (20%), affection (20%), positive (20%), perception (20%), visual (20%), relative (40%), and time words (40%). LIWC has been used in numerous studies, covering a wide range of topics which included predicting deception from textual words [12], identifying gender differences in language

use [13] and the use of language to identify personality styles [14]. It was also used to reveal the psychological changes in response to an attack, for example, the terrorist attack on 9 September 2001 that destroyed the Twin Towers in the United States of America [15].

Style features can also be used to identify writing style. The four major categories of style features are: lexical, syntactic, structural, and content-specific [16]. Lexical features include total number of words, words per sentence, and word length distribution. Syntax refers to the patterns used for the formation of sentences, such as punctuation and function/stop words. Structural features deal with the organization and layout of the text, such as the use of greetings and signatures, the number of paragraphs, and average paragraph length. Content-specific features are keywords that are important within a specific topic domain.

### 2.3 Terrorists Uses

Terrorists also uses social networking sites. At the University of Arizona Dark Web Terrorism Research Centre, complex models have been built to study extremist-group web forums and thus construct social network maps and organization structures. Research has been carried out to analyze social networking sites but terrorists could also use networking sites to their advantage [17]. Work conducted by Veerasamy and Grobler [18] discussed the different methods used by these organizations for recruitment. The use of profiling techniques could allow these groups to identify potential members based on their psychological characteristics revealed through their expressive writing.

Social networking analysis enables multi-variant analysis which is important for terrorism as the combination of multiple factors: for example, poverty and type of government, combined with the link to a terrorist, may cause a person to participate in a terrorist activity [17]. Thus, using linguistic analysis to gauge these various factors can be beneficial into determining a person's potential to be recruited into a terrorist organization. Furthermore, Ressler says that social network analysis should try to understand the underlying root of terrorism and therefore it is useful to understand how terrorist networks recruit participants and why people join terrorist organizations [17]. By studying the social engineering approaches based on linguistic analysis, insight can be gained on terrorist recruitment practices.

Recruitment could further be extended to include insiders, who are people within companies whom are trusted and have authorized access to valuable resources [19]. The recruitment of insiders employed at critical infrastructure<sup>1</sup> establishments could have devastating effects on the services required to operate a country and could constitute a national security risk. The next section describes the process implemented to protect the identity of the users during the data harvesting.

---

<sup>1</sup> The facilities which are essential for the functioning of a society and economy for example financial services, transportation systems, water supply, public health, etc.

## **2.4 Method of Data Collection**

This study only collected data to demonstrate a possible information gathering phase of a social engineering attack. The only contact made with users was the use of the ‘friend request’ from Facebook to determine the rate of accepting requests without verifying the true identity and purpose of the request. The friendship was terminated once a request was accepted. Also the data analysis was used to determine potential victims based on emotional response to content; no mechanisms were used to test the findings. No automated tools were used in the data collection as this would transgress the social networking sites the terms of use.

## **3 Proof-of-Concepts**

This section describes the proof-of-concept to determine what data could be gathered from responses on social news sites and how it could be used to conduct a social engineering attack.

The process of a social engineering attack consists of three phases: identify a potential target, data collection to understand and find weaknesses within the target and finally exploit the vulnerabilities identified [20]. This experiment followed the same phases. The design of the experiment involved the manual collection of data from a social media news site, which will not be identified in this paper. The web articles published on this site were selected with the criteria of most responses in the form of posts and comments. This site allows users to post responses to published articles and add comments on posts from other users. Users who would like to create responses are required to login using Facebook account credentials or can create an account on the site.

The user’s response in the form of a post or comment can be extracted including the user name and a URL link to their personal profile. The collection process involved the manual capturing of comments and posts from articles published on the site. The collected information does not consist of any personal information except for the URL of the profile which is not revealed in this paper. The collected data were used in two experiments. The first experiment determines what information can be collected using the profile data collected and the second experiment what information can be deduced from the responses created by the users. These two experiments are explained in the following sections.

### **3.1 Data Collected on Profile Information**

A list of all the unique users with their URLs who created responses were compiled from the data collected. Each of the user’s profiles was visited to determine how much data was available. A summary was created to illustrate the following categories: visibility of the activities and interests, listing of friends and contact information. The activities and interests could help social engineers in creating a profile about the



user. The summary lists the availability of each of these categories from the public domain (not logged in) and when authenticated (logged in).

The process involved using two web browsers. Facebook was opened in both browsers. In the one browser, which a Facebook user was not logged into, the URL of the collected profile was opened in the browser and subsequently the availability of the required categories was captured. The other browser used the same process except that it used a valid Facebook account and logged into Facebook before opening the collected profile URL. In brief, data was collected about availability of information on a Facebook profile when logged in and not logged in. Next a friend request was sent to the collected profiles. The status of the friend request was also recorded. The status conditions are defined as requested, accepted, not enabled and message. There are no responses sent to the requestor if the friendship request is declined, hence no state is created to indicate declined friendship requests.

The different conditions were explained in Table 1. The friend requests are used to determine the current susceptibility of users to accept friend requests without verifying the trustworthiness of the user who sent the friend request.

**Table 1.** Status Description

<b>State</b>	<b>Description</b>
Requested	A friend request has been sent and is pending
Accepted	The friend request has been accepted
Not Enabled	Friend request feature disabled by user
Message	Friend request was not accepted but message was sent from user

### **3.2 Data regarding Users Responses**

The captured responses from the users on the social news website were captured in a database. Some information could be inferred by visiting the profile associated with each user. This experiment analyzes and investigates how the textual responses could be used for profiling as part of a social engineering attack. The data within the database is converted into a text file which is used by LIWC to determine the different emotional dimensions including anger, positive, negative. All of these could be used to determine personality traits. A results file is created once the text files have been processed. The content of the resulting file is extracted and stored in a database which correlates with the previous collected data. This allows the research team to have access to the collected and analyzed data.

Social engineers could use the same process after the collection phase is completed to determine gender. Males have been shown to use more articles (a, the), nouns, prepositions, numbers, words per sentence and use more swear words than females [21]. In this paper we identify negativity and anger as these two emotional states could be employed during a social engineering attack. The use of words could provoke anger in a person which subsequently would prevent the user from making logical decisions [22]. The analyzed data could identify users on social networking sites

who are prone to anger; as the high use of negative and anger words could leak this information unknowingly to cyber criminals.

## **4 Findings**

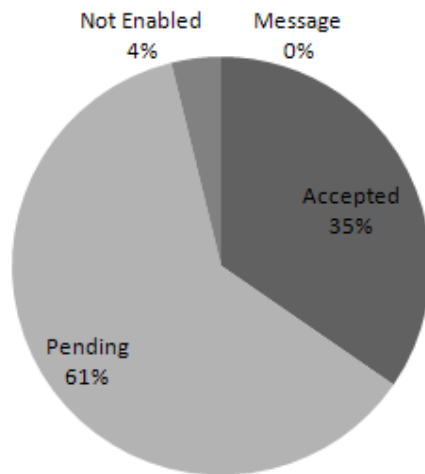
In this section we describe the results from the experiments conducted. This includes information about the data collection method, the findings from the friendship requests and the analysis of the responses collected.

### **4.1 Data Collection**

The following section describes the finding of the two experiments described in Section 3. A total of 353 unique profiles were listed from the sample collected which consisted of 791 comments and 728 posts from nine articles published on the news website. Data was collected and subsequent friend requests were sent to each user. No additional interactions were conducted after the friend request was sent. A total of 130 requests were sent to users over a period of three days. However, Facebook issued a warning after some users reported the friend requests as suspicious behavior. Consequently, we ceased the friendship requests action. The high acceptance rate was noticed within the first week and then declined after the second week. The collection period spanned over four weeks to ensure that most users had the opportunity to accept the friendship requests sent to them. Security measures implemented by Facebook delayed the collection process using the web browser without having logged into Facebook. Facebook uses mechanisms to identify automated tools and forces the users to prove human behavior with a text challenge e.g. Captcha, before allowing the user to continue. Thus Facebook presents a question and the user must provide a valid answer to be proceed.

### **4.2 Analysis of Profile Information**

This section describes the findings from the information gathered using only the profile URL collected. Findings specifically addressing the friendship requested, are depicted in Fig. 1. At the time of writing the following statistics are available from the data collected. A 35% success rate of friendship requests accepted was obtained from the 130 friend requests sent to the users. Only 4% of users did not enable the “Send Friend Request” feature thus preventing other users from requesting a friendship. An interesting observation is that no users who accepted friendship requests sent messages to request additional information from the unknown user to establish trustworthiness.



**Fig. 1.** Facebook Friend Requests

Findings on the data leaked from the profiles are depicted in Fig. 2. Analysis of the data gleaned from the profiles indicates 59% of profiles leak information about interests and activities without the need to log into Facebook. In addition, logging into Facebook and then viewing the profile reveals 79% of interests and activities, an increase of about 20%, compared to the public view of a profile. Equally important is the availability of the user's friends listing which indicates an increase of about 70% of visibility when using a logged in Facebook session. The availability of contact information does indicate a slight increase when accessed through a logged in account.

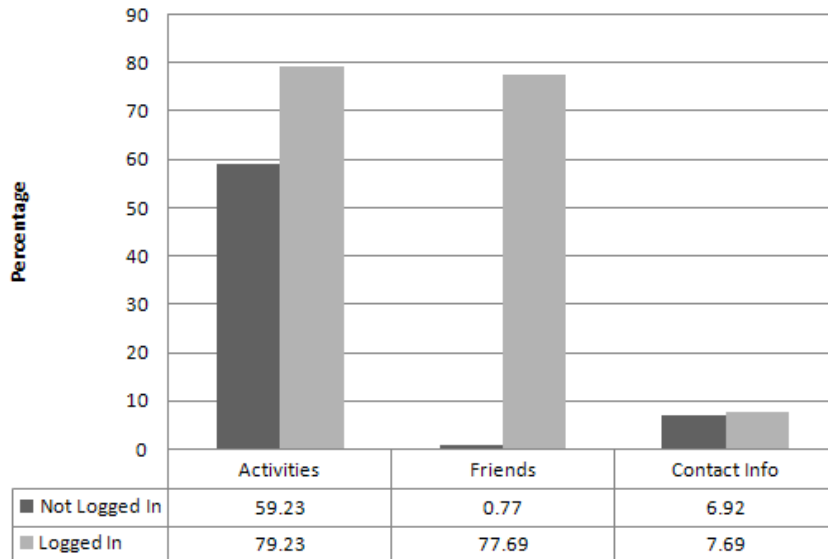
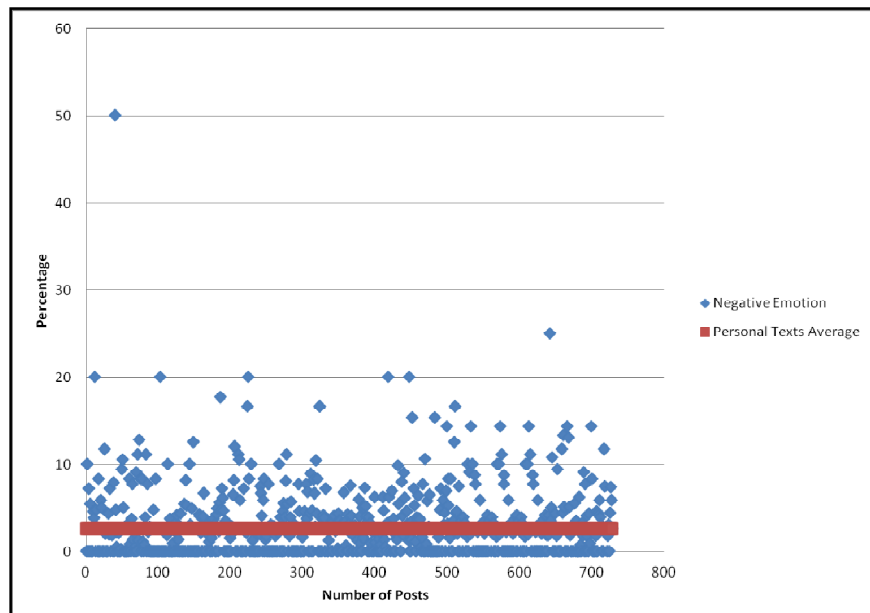


Fig. 2. Data Leakage

### 4.3 Analysis of Users Responses

The following section discusses the findings to determine if any users have leaked information which would profile them as prone to a social engineering attack using an emotional trigger. Thus, a form of content-specific writing style analysis was carried out. All the posts and comments were processed to determine the overall average negativity. These include but are not limited to the following negative emotion words: arrogant, ineffective, cheating, outrage and shock. The average negativity of the posts was calculated as 2.9% whereas the average negativity of the comments was calculated as 3.03%. This could be due to human nature where people are more reactive to what other people say or write. Posts were responses on an article which was written impartially. However, comments are responses to bias posts. According to research by Pennebaker, the mean use of negative words in personal text, written to express an opinion, is 2.6% [23]. This indicates the existence of posts and comments with a high frequency of negative words.

Fig. 3 provides a graphical representation of the analyzed posts with the mean included. One outlier was identified in the results. The 50% post, upon inspection was a two word sentence with one word a negative word and is subsequently not used in the findings. In addition, numerous posts are clearly more negative than the mean average. The writer of these posts can be classified as potential victims by social engineers. The identity of the potential victim could be extracted from the collected data to initiate an attack. No limiting parameters were utilized during the search hence producing a large potential victim set.



**Fig. 3.** Negative Emotions for Posts

In addition, the anger dimension was analyzed from the 728 posts collected. The analysis parameters were set to only include posts with a higher percentage than 10%, thus producing a smaller victim pool which will be more susceptible to a social engineering attack (See Fig. 4).

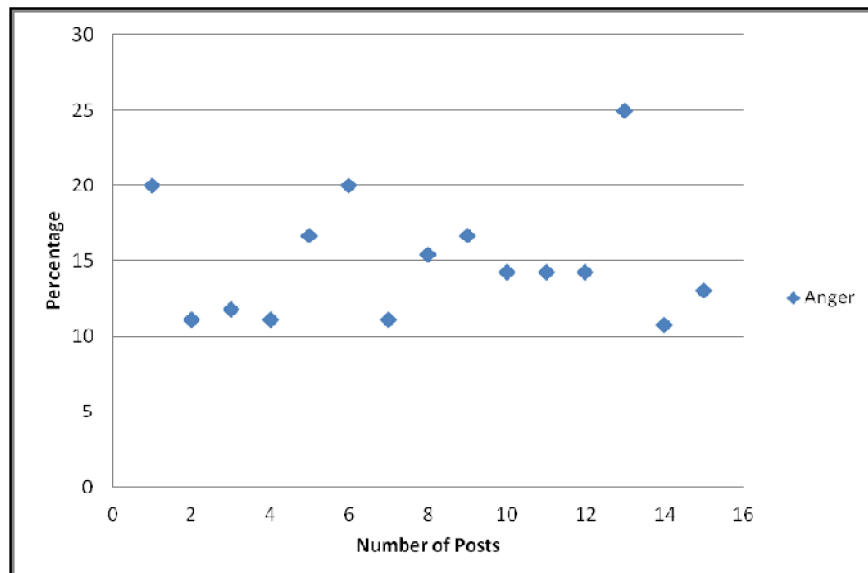


Fig. 4. Anger Emotions above 10%

## 5 Discussion of the Experiment

In this section we discuss the results found in Section 4 and how the information could be used for malicious intent. Access to users' information could potentially allow attackers to utilize a wide range of methods for nefarious use. Also the collection and analysis of responses could assist in a successful social engineering attack.

### 5.1 Using Profile Information to Access Additional Data

The information inferred from using only the URL of the user's profile, found users do not understand the mechanisms provided by Facebook to prevent the leaking of personal data. The privacy control settings are continuously updated by Facebook, adapting both to new features developed by Facebook and to the ever changing threat in the environment. However, according to a study by ProtectMyID it was found that only 18% of users implement privacy setting controls [24]. This implies that attackers could easily harvest personal data about users without the need to bypass security measures implemented by social networks.

The results of this study found that more is available when accessing a profile that has once logged onto Facebook. Also most users make public their friend lists which could be used by social engineers to conduct an attack using an evil twin attack. An

evil twin attack is defined as using a rogue profile<sup>2</sup> to impersonate a legitimate profile [25]. The attacker could use data collected from a friend of a Facebook user to create a similar profile to that of the actual friend and subsequently make a friend request. The victim could implicitly trust the source based on the familiarity of the “friend” making the request and information provided with the request which could include a picture and the name of a trusted friend. Another concern raised by the results of this study is the friend request acceptance rate. The study showed that users accept 30% of friend request without asking for additional information.

## 5.2 Profiling Users

Responses created by users to raise their opinions on current news events could also be used by social engineers. Some of users’ personal traits are leaked by expressing an opinion on a specific topic. The use of tools which conduct linguistic analysis could be used to profile a user.

Profiling takes two approaches: prospective and retrospective [26]. Prospective profiling involves the development of a template from previous data. The developed template is then applied to future data to identify individuals whom resemble the characteristics defined within the template. Retrospective profiling uses data left behind to develop a description of the user. In this study retrospective profiling using the data created by the users on the social networking site was used. Such profiling could be used by social engineers to design an attack with elements that improve the probability of a successful attack. The results from the data collected in this study demonstrated how anger and negative emotions could be determined from the responses collected. From this data the attacker could extract the original post that would determine the content which provoked the emotion. This could be then used in designing a customized social engineering attack such as a spear-phishing attack. This attack is targeted towards a specific person or group. The use of this information in a possible social engineering attack is describes in the next section.

## 6 Application of Data Collected to Conduct a Social Engineering Attack

An attacker could inspect a social news website for controversial articles which have the most responses. Next the attacker collects the data in the form of responses and analyzes these to determine which users have demonstrated the most positive or negative emotions towards an article. These users are classified as victims. The attacker has implicit access to the Facebook profiles of the victims. The attacker uses a fake profile to access data on the individual victim’s profile. Results from our study have shown a high probability to access the list of friends. The attacker next uses an evil twin attack and creates a Facebook profile to impersonate one of the friends from the victim’s friend list. Next the attacker creates a malicious PDF, naming the file to

---

<sup>2</sup> Profiles with information which creates a false sense of trustworthiness

correlate with the topic which generated the emotion. For example the analysis showed that the target is negative towards a new tax which will be introduced into the victim's country. The attacker then uses the mail functionality of Facebook to attach the malicious PDF to a Facebook message. The attacker next creates an enticing message using the topic. For example: "*Shocking information leaked about the controversial tax*". The victim will receive the message with the malicious PDF from the fake profile which has the same profile picture as a trusted friend. The victim could implicitly trust the source and then due to the emotional trigger be influenced to open the malicious PDF and infect their systems with malware.

## 7 Future Work

In this experiment, users were invited to become friends in a social networking site based on a legitimate profile. The experiment will be repeated with the same sample group and the response compared to an invitation from a profile that has minimal information and thus could appear to be an illegitimate user. Thus, a comparative study will be carried out to determine whether users' responses are similar when the profile invitation differs in terms of its degree of legitimacy. This will indicate the need to address the identification of fake profiles on social networking sites.

In addition, this paper briefly introduced the use of linguistic analyses for terrorism recruitment practices. Further research will be carried out to conduct linguistic analyses on social networking sites to determine patterns with relation to content, language and style.

## 8 Conclusions

In this paper we addressed how users' digital footprints in the form of responses on social news website can be used to create additional attack vectors that could be used to target them.

Two experiments were carried out to determine whether a user could be profiled from their posts on social news sites and also to investigate users' awareness of privacy control settings on social networks. The results show that users can be naive and have a false sense of security which encourages behavior that exposes them to threats. This could be mitigated with security awareness training which allows users to understand the purpose of privacy setting controls and how to implement these to protect personal information on social networking sites. The training could also include other threats that could be encountered on social networking sites for example the evil twin, social engineering and phishing<sup>3</sup> attacks. Furthermore this study showed how emotional triggers that influence users could be determined from responses collected within the public domain. The users should implement strategies to protect their identities on social networking sites which promote freedom of expression. For example, the user could create an alternative profile specifically used to participate on forums

---

<sup>3</sup> To try to obtain financial or other confidential information from Internet users [27]



which allow users to raise their opinions. These profiles should contain no information which could be used identify the identity of the user.

Both the methods used in this study could be used by social engineers as part of the information gathering phase. The research revealed that information exposed in social networking platforms could be used for nefarious purposes like retrieving personal information, as well as profiling. Furthermore, the personal information that is obtained through the social engineering techniques could be used in an advanced attack vector which combines multiple attack mechanisms to circumvent protective measures implemented to secure a system. In addition, the work has shown that the profiling techniques could be used for malicious purposes like terrorist recruitment and the identification of insiders within critical infrastructure which poses a significant threat to national security. For example, these attackers could target critical infrastructure by identifying possible individuals to infect with malware which targets the critical infrastructure systems or recruit the individuals to join the cause of the terrorist group. These new infected systems or the recruitments could be dormant until action is required by the terrorist group. The access to personal information in the public domain enables these groups to devise strategies to identify and recruit members. These members could be recruited during the planning phase of a possible attack against a country and subsequently become active participants during the execution of the planned attack. Individuals in positions which can cause catastrophic damage to the national security of a country should be cautious of information posted in the public domain. The use of security awareness training that focus on the dangers of personal information in the public domain could provide these individuals with mechanisms to protect themselves against the threats identified. This paper thus aims to create awareness about the dangers of the inference of personal data in the public domain.

## 9 References

1. I. Mann, *Hacking the Human*, Gower Publishing Ltd, (2008).
2. C. Carl, "Human factors in information security: The insider threat – Who can you trust these days?" *Information Security Technical Report*, vol. 14, pp. 186-196, (2009).
3. C. Hadnagy, *Social Engineering: The Art of Human Hacking*, Wiley, (2010).
4. D. Shinder. (2010). Profiling and categorizing cybercriminals. Available: <http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069>. Last accessed 11 Feb 2012.
5. D.C. Evans, S.D. Gosling and A. Carroll, "What elements of an online social networking profile predict target-rater agreement in personality impressions," in *Proceedings of the International Conference on Weblogs and Social Media*, pp. 1-6, (2008).
6. C.K. Chung and J.W. Pennebaker, "The psychological function of function words," *Social Communication: Frontiers of Social Psychology*, pp. 343-359, (2007).
7. J.B. Hirsh and J.B. Peterson, "Personality and language use in self-narratives," *Journal of Research in Personality*, vol. 43, pp. 524-527, (2009).
8. T. Ryan and S. Xenos, "Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage," *Journal of Computer Human Behavior*, (2011).

9. M. Vollrath and S. Torgersen, "Personality types and coping," *Personality and Individual Differences*, vol. 29, pp. 367-378, (2000).
10. D.Vergano. (2011). Terrorists taunts may tell attack. Available: [http://www.usatoday.com/tech/science/columnist/vergano/2011-02-27-terrorist-words\\_N.htm](http://www.usatoday.com/tech/science/columnist/vergano/2011-02-27-terrorist-words_N.htm). Last accessed 27 Feb 2012.
11. J.W. Pennebaker, R.J. Booth and M.E. Booth, "Linguistic inquiry and word count (LIWC2001): A computer-based text analysis program." (2001).
12. M.L. Newman, J.W. Pennebaker, D.S. Berry and J.M. Richards, "Lying words: Predicting deception from linguistic styles," *Person.Soc.Psychol Bull.*, vol. 29, pp. 665-675, (2003).
13. M.L. Newman, C.J. Groom, L.D. Handelman and J.W. Pennebaker, "Gender differences in language use: An analysis of 14,000 text samples," *Discourse Processes*, vol. 45, pp. 211-236, (2008).
14. J.W. Pennebaker and L.A. King, "Linguistic styles: Language use as an individual difference." *Journal of Personality and Social Psychology*, vol. 77, pp. 1296-1312, (1999).
15. M.A. Cohn, M.R. Mehl and J.W. Pennebaker, "Linguistic markers of psychological change surrounding September 11, 2001," *Psychological Science*, vol. 15, pp. 687-693, (2004).
16. Y.D. Chen, A. Abbasi and H. Chen, "Framing Social Movement Identity with Cyber-Artifacts: A Case Study of the International Falun Gong Movement," *Security Informatics*, pp. 1-23, (2010).
17. S. Ressler, "Social network analysis as an approach to combat terrorism: Past, present, and future research," *Homeland Security Affairs*, vol. 2, pp. 1-10, (2006).
18. N. Veerasamy and M. Grobler, "Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure," in *Leading Issues in Information Warfare & Security Research*, pp. 172-187, (2011).
19. S.E. Goodman, J.C. Kirk and M.H. Kirk, "Cyberspace as a medium for terrorists," *Technological Forecasting and Social Change*, vol. 74, pp. 193-210, (2007).
20. N. Barrett, "Penetration testing and social engineering: Hacking the weakest link," *Information Security Technical Report*, vol. 8, pp. 56-64, (2003).
- 21] J.W. Pennebaker, *The Secret Life of Pronouns: What Our Words Say About Us*, Bloomsbury Press, (2011).
22. R. Brodie, *Virus of the Mind: The New Science of the Meme*, Hay House Publisher, (2011).
23. J.W. Pennebaker, C.K. Chung, M. Ireland, A. Gonzales and R.J. Booth, "The development and psychometric properties of LIWC2007," Austin, TX, LIWC.Net, (2007).
24. C. Whitlock. (2011). New survey data from Experian's ProtectMyID™ reveals people are making it easy for cybercriminals to steal their identity. Available: <http://www.prnewswire.com/news-releases/new-survey-data-from-experians-protectmyid-reveals-people-are-making-it-easy-for-cybercriminals-to-steal-their-identity-131441283.html>. Last accessed 10 Oct 2011.
25. C. Timm, "Evil Twin Attacks," in *Seven Deadliest Social Network Attacks*, Syngress, (2010), pp. 63-82.
26. N. Nykodym, R. Taylor and J. Vilela, "Criminal profiling and insider cyber crime," *Digital Investigation*, vol. 2, pp. 261-267, (2005).
27. Anonymous "The Free On-line Dictionary of Computing," (2012).

## **Design of a cyber security awareness campaign for Internet Café users in rural areas**

WA Labuschagne<sup>1</sup>, MM Eloff <sup>1</sup>, N Veerasamy<sup>2</sup>, L Leenen<sup>2</sup>, M Mujinga<sup>1</sup>.

<sup>1</sup>School of Computing, Unisa

<sup>2</sup>Council for Scientific and Industrial Research

[wlabuschagne@csir.co.za](mailto:wlabuschagne@csir.co.za)

[eloffmm@unisa.ac.za](mailto:eloffmm@unisa.ac.za)

[nveerasamy@csir.co.za](mailto:nveerasamy@csir.co.za)

[lleenen@csir.co.za](mailto:lleenen@csir.co.za)

[mujinm@unisa.ac.za](mailto:mujinm@unisa.ac.za)

**Abstract:** Africa may have the lowest number of Internet users in the world, but it also has the highest growth rate and the number of users is steadily growing. A majority of the African population is still excluded from global cyber networks and thus have very low cyber literacy rates. A consequence of these two factors is that many Internet users access the Internet without understanding or even realising the dangers of the cyber world. Proactive measures need to be developed to ensure that these new Internet users are equipped with computer and information security knowledge to mitigate possible cyber attacks.

Due to limited availability of infrastructure, a large percentage of the African population access the Internet via Internet Cafés. A need has been identified to make users aware of the threats that may be present at an Internet Café. This paper addresses how the National Institute of Standards and Technology (NIST) framework, defined in the guide, “Building an Information Technology Security Awareness and Training Program”, can be used to develop a security awareness program that focuses on possible cyber threats at Internet Cafés. This guide provides a framework that can be applied to construct a security awareness program. It consists of four steps that form part of the life cycle of an information technology (IT) security awareness and training program. These steps are used to identify requirements of a security training strategy, to develop material that addresses the identified requirements, for the effective roll-out of the program, and to ensure the program is current and to monitor the effectiveness of the program. This framework can be used to address an identified threat in a specific context. This paper addresses the development of a security awareness campaign with the focus on reducing threats emanating from Internet Cafés.

**Keywords:** cyber attacks, cyber literacy, cyber threats, Internet Cafés, security awareness, security training.

### **1. Introduction**

Africa lags behind the rest of the world in terms of basic telecommunication and computing infrastructure, which results in poor connectivity rates compared to non-African countries. The digital divide refers to the gap between those with regular effective access to digital technologies, particularly the Internet, and those without [7]. Globally, the digital divide describes the gap between economically developed and developing countries, but on a national level, the digital divide often results in an urban-rural divide. In poor countries, and particularly in rural areas, most people can only gain access to the Internet through public access points such as Internet Cafés. Internet Cafés usually provide relatively inexpensive Internet access to people who cannot afford personal computers and often are unemployed.

Mutula [19] affirmed that the poor telecommunications infrastructure in Africa can be attributed to a number of factors, including governmental policies. Most African governments reluctantly freed up their telecommunications services although some still regulate these services. Regulation often hinders private companies to obtain licences to provide telecommunications services. Other factors

include language barriers, lack of awareness, costs, and poor connection speeds. Mutula also mentions initiatives by the South African government to deliver affordable technology.

Otieno reported in 2010 that Africa has the lowest number of Internet users in the world. This problem prevents the majority of Africans from enjoying the benefits of digital media [21]. The current estimated statistics provided by Internetworldstats.com show the current Internet users from the African continent contribute 5.6% to the total number of Internet users in the world [12]. Furthermore, during the past decade, the number of Internet users from the African continent has grown at a rate of over 2000% [12]. These low figures could be explained due to the high cost and the limited availability of infrastructure in Africa. Twinomugisha identified the lack of infrastructure in Africa resulting in low bandwidth and high costs [25]. Africa thus has the lowest number of Internet users in the world, but it also has the highest growth rate and the number of users is steadily growing. This growth has led to new requirements with regards to the development of infrastructure: the roll-out of the Seacom, EASSY and TEAMS cables has significantly increased bandwidth in the African continent [25]. The SEACOM and TEAMS cables were launched in 2009 and the EASSY cable in 2010 [23] [3] [24]. Usage at Internet Cafés is likely to also increase due to the increasing availability of infrastructure. However, a large majority of the African population is still excluded from global cyber networks and has very low cyber literacy rates. Milicevic reported that more than 80% of the population of the planet is literally excluded from global information networks that provide economic, cultural, political and social interaction [17].

These factors contribute to a situation where a large number of Internet users access the Internet without knowing or even understanding the dangers of the cyber world. Proactive measures need to be developed to ensure that these Internet users are equipped with computer and information security knowledge to mitigate possible cyber attacks. In less affluent areas, the cost of Internet access and the lack of monetary means to purchase a personal computer has resulted in limited home based Internet access. A growing challenge is the creation of cyber security awareness in rural areas for Internet Café users and establishing a way through which awareness can be increased.

A security concern, for which awareness needs to be created, is the spread of malware. The nature of malware is to lure users, through the web browser used at Internet Cafés, into performing an action which will then infect the system [22]. Polychronakis et al. also noted that 68% of the users make use of portable storage devices [22]. These devices are a main attributable factor in the spread of malware. The study also revealed there is a high demand for formal training courses to educate rural users on good security practices and the dangers of malware. Security measures implemented by employers are another important factor, identified by Kritzinger and von Solms [14]. Most corporate employees are protected by mechanisms deployed by their company to protect the users against cyber threats. In most instances these users attend computer and information security awareness programs to help them understand possible cyber attacks that they may be exposed to. A large number of companies have budgets to ensure that the best possible measures are deployed to protect their assets. On the other hand, Internet Café owners generally do not provide the same level of protection or training.

This paper addresses how the National Institute of Standards and Technology (NIST) framework, defined in the guide: "Building an Information Technology Security Awareness and Training Program", can be used to develop a security awareness program that focuses on cyber threats identified at Internet Cafés. National Institute of Standards and Technology (NIST) is an agency of the United States Department of Commerce. NIST developed this Special Publication 800-50, which provides guidance for building an effective information technology (IT) security program [26]. This guide provides a framework that could be used to conduct a successful security awareness program; it addresses four critical phases that form part of the life cycle of an IT security awareness and training program. These phases are used to identify a need for a security training strategy, the development of material that addresses the identified needs, the effective roll-out of the program and steps to ensure the program is current and monitors the effectiveness of the program.

The remainder of this paper is structured as follows: Section 2 gives some background on Internet Cafés in rural areas, Section 3 discusses the NIST framework, Section 4 considers issues surrounding security awareness levels of Internet Café users, and in Section 5 the NIST guidelines are applied to develop a framework for a security awareness campaign for Internet Café users in rural areas. Section 6 concludes the paper.

## 2. The Internet Café Industry in Africa

An Internet Café is a privately owned business that provides access to the Internet, as well as the usual services of a traditional café such as coffee and snacks. The first Internet Café was opened in London in 1994 [2]. In the United States, a business that provided coin-operated computers with dial-up access to the Internet was launched as early as 1991. The first actual Internet Café in the US opened in 1995 in Chicago.

Hyde-Clark [11] claims that the first South African Internet Café, The Milky Way Café, was opened in Johannesburg in December 1994. Limited statistics regarding growth rates and current numbers of Internet Cafés in Africa exist, but we give a short summary of a few relevant studies. Mutula [19] reported in 2003 that there was significant growth in the industry in South Africa from 1999. Molowa [18] also notes that the industry is growing at a high rate in South Africa, but he does not provide statistics. Mwesige [20] notes that Uganda has seen a rapid growth of Internet Cafés, although at the time of this report, the growth was mostly in the capital city, Kampala. The first Internet Café started in 1996 in Uganda.

There are a number of studies on the nature of Internet Cafés and their users in rural and urban areas, as well as in affluent and poorer areas. A few examples from these studies are provided in the following paragraphs.

Two studies that focus on Internet Cafés in Johannesburg cite differences in the Internet usage and costs in affluent and poorer areas. Hyde-Clarke [11] compares two Internet cafés and notes that the rates charged by the Internet café in the more affluent area are significantly higher than the café in the poorer area. He also notes that users in the more affluent area mainly use the Internet to expand existing business activities, while users in the poorer areas tend to use the Internet to search for employment or to attempt to establish business contacts. In addition, Hobbs and Bristow [10] studied a number of Internet Cafés in both affluent and less affluent areas in Johannesburg. They found that there are more Internet Cafés in less affluent areas. This is likely because poorer people are less likely to have their own personal computers. Another observation is that 64% of users in the study used more than one Internet Café, and that 65% of users have a high rate of repeat usage. Another important observation is that there is a high demand for training at cafés and that fellow users often offer assistance or informal training to less competent users, or that some users access the Internet on behalf of other people who do not have the required skills.

From a wider perspective, Furuholt and Kristiansen [7][8] studied Internet Cafés in Indonesia and Tanzania and compared the industry in these two developing countries. They also note that in developing countries, most Internet users gain access to the Internet through public access points such as Internet Cafés. In their study on cafés in Tanzania they found that there are 16 times more people per Internet Café in rural areas than in urban Dar es Salaam. They also find that rural users on average have one third of the income of their urban counterparts, but they spend almost the same amount of money at Internet Cafés. In their comparative study of Tanzania and Indonesia, they found that although these two countries are at different levels of development, their Internet Café users are remarkably uniform. In both these countries, Internet Café users tend to be poor but spend a high percentage of their income on Internet Café services. The main activity is to read and write emails, but the cafés serve a role as training facilities. Internet Café staff can therefore be used to provide training and awareness to less educated people.

Furthermore, Mwesige [20] reported in his study of Internet Cafés in Uganda that very few residents owned a personal computer and access to the Internet is mostly provided by public access points such as Internet Cafés. He also reported that repeat usage is very high in Uganda and that users in cafés mostly accessed their email.

Overall, Furuholt and Kristiansen [8] give an overview of studies on the industry globally, but the results that are relevant in our context support the observations we mention above. These observations are relevant to an awareness campaign because:

- The Internet Café is often the only access point for a rural, poorer person. Such a user is possibly unemployed and may not have had exposure to security awareness campaigns.

- There exists a need for training at Internet Cafés and this requirement implies that there probably exists a lack of cyber security awareness. A high percentage of Internet Café users are repeat users. Repeat users can contribute to reliable participation in an awareness campaign. If we apply this trend to the generally less affluent rural environment, we can conclude that decentralised Internet access exists and this could affect the reach and impact of an awareness campaign.

It has been identified that the NIST framework would serve as an ideal guide to implement an awareness campaign for Internet users in rural areas. In the next Section, a high-level overview of the NIST framework is provided.

### **3. The NIST guide to develop a Technology Security Awareness and Training Program**

The National Institute of Standards and Technology has developed a framework that aims to guide the development of an Information Technology (IT) security program. In this study, the framework is used to design a campaign to create cyber security awareness in Internet Cafés in rural areas. This Section contains a summary of the NIST framework so as to provide the context for the work in the other sections [26].

The NIST framework consists of four high level steps. Figure 1 shows a summary of the relevant steps of the NIST framework to guide the development of a cyber security awareness campaign. A short summary of each step follows.

#### **3.1 Designing an Awareness Program**

To design an awareness program, a needs assessment needs to be carried out. The following issues pertain to a needs assessment:

- A needs assessment is a process that can be used to determine an organisation's awareness needs.
- It is important to consider the motivation and methodology to conduct a needs assessment.

The outcome of a needs assessment is an understanding of security issues that will help shape the strategy and design of the IT security awareness program.

#### **3.2 Developing Awareness Material**

The issues to consider when developing awareness material are the selection of the awareness topics, as well as the sources of developing the awareness material. The development of the awareness material is dependent on the needs assessment. The needs assessment will identify the topics which need to be addressed when developing the awareness material.

#### **3.3 Implementing the Awareness program**

To implement the awareness program, a selection will be made of the techniques through which the messages will be delivered. The chosen techniques will depend upon resources and the complexity of the messages. Techniques for effectively delivering training material should take advantage of technology that supports:

- Ease of use;
- Scalability;
- Accountability;
- Broad base of industry support.



**Figure 1: High-level outline of NIST framework**

The different means of transferring security knowledge are through the use of formal training sessions, strategic placement of awareness messages, passive computer-based, web-based, and interactive computer based training. Problems have been identified to hold a user's attention due to the passivity of the knowledge transfer. Formal training sessions can be conducted by an instructor who will use material like books and presentations to transfer the content to the users. This method does not involve the participation of the user and is usually seen as one-way communication. The knowledge attained during these types of sessions may be quickly forgotten once the sessions are completed. Computer based training is where the user is exposed to the information via a computer and learning is conducted in their own time. Knowledge is only transferred to the user and the application of the knowledge is never used in real applicable situations. This does not imply that the knowledge gained will be retained over a long period or will be applied in a situation whereby the knowledge would be useful to resolve a problem.

The use of awareness messages is helpful to make people aware of certain knowledge. This can be done with the use posters, screen savers or emails that contains security related information. However, similar to computer based training methods, the publication of awareness messages does not imply that the knowledge is retained or guarantees that the information was understood.

A good method to transfer and provide a platform where the information can be useful, is with the use of interactive computer based training. It provides information and ensures that learning does take place, due to the active interaction. This medium can ensure that knowledge gained is used in the right context in the right environment. The trainee can obtain immediate feedback based on the actions required to solve a problem. Video games are interactive computer based training, and examples include CyberCIEGE and CyberProtect. Both these tools can be used to transfer cyberspace security knowledge.

Thus, during the implementation of the awareness program, a decision will need to be taken with regards to the delivery method. Issues regarding interaction requirements and retention strategies will be taken into consideration.

### **3.4 Post-implementation**

During the post-implementation phase, the security awareness program can be evaluated. Once the program has been implemented, processes must be put in place to monitor compliance and effectiveness. The feedback loop provides a strategy to ensure that the program continues to be relevant and compliant with the overall objectives. Continuous improvement cannot occur without a good evaluation of how the existing program is working. Assessments after an awareness campaign can be used to determine if any knowledge has been effectively acquired during the learning process.

### **3.5 Summary**

This section provides a short summary of the NIST framework. It highlights the main phases to be implemented when designing a security awareness program. The next section addresses the application of the NIST framework to the design of a cyber security awareness campaign for Internet Café users in rural areas.

## **4. Design of a Cyber Security Awareness Campaign**

In this section, we apply the NIST framework to design security awareness program for Internet Cafés in rural areas. Each of the steps described in Section 3 will be applied sequentially, in order to explain how a cyber awareness campaign for Internet users in rural areas can be developed. The initial step is the completion of a needs assessment to initiate the design of the awareness campaign. The description of the needs analysis follows in the next section.

### **4.1 Conducting a Needs Assessment**

With reference to Figure 1, the initial step in the NIST framework is the Design of the Awareness Program. This is achieved through a needs assessment. The needs assessment process can be carried out by:

- Interviewing Internet Café owners.
- Literature study of attack vectors at an Internet Café.
- Observation and identification of threats.

Threats are considered as the source/person/organisation that seeks to breach security and benefit from an exploitation attempt. An attack vector is the medium through which the threat is exploited and can thus be considered as a vulnerability or weakness of the system. Attack vectors are relevant as they will be used in the development of awareness material when the means through which a threat can be exploited, will be explained to the user. Therefore, it is essential to consider both the threats and the attack vector. Core to the needs assessment and the completion of attack vectors is a literature study to identify threats and Internet uses.

#### **4.1.1 Identification of Internet Uses**

Furuholt & Kristiansen discuss the various uses of the Internet [9] [7]. In order to complete the mapping of the attack vectors covering threats and Internet uses, the findings of Furuholt & Kristiansen are further classified as a means of abstraction for future application. Social Networks are included as an additional Internet use. Table 1 was generated by listing Internet uses and then



classifying a use into a high-level categorisation. This provides a level of abstraction for the compilation of the mapping of attack vectors.

**Table 1: Internet Use Classification**

Type of Use	Classification
Seeking information	Information
Email	Communications
Chatting	Entertainment
Reading online news	Information
Research	Information
Computer games	Entertainment
Downloading software for professional use	Business
Downloading software for amusement	Entertainment
Downloading music	Entertainment
Visiting pornographic sites	Entertainment
Doing business	Business
E-shopping	Financial
Gambling	Financial
Social networks	Communications

#### 4.1.2 Identification of Threats

The use of the Internet is far-ranging and spans functionality from communication to entertainment. Such functionality also brings with it associated threats that can be exploited and should therefore be considered in a needs assessment. A literature study on Internet threats in rural areas is therefore carried out next.

Firstly, the works of Anselmi, Menon, Won, Evans and Manning are considered collectively. Identified threats include: worms, Trojans, password/info stealers, adware, backdoors, viruses, exploits, spyware, phishing, downloaders, droppers, ransomware, social engineering and rootkits [1] [16] [13] [4] [15].

Furthermore, the works of Akhil and Evans also discuss threats like browser based attacks and social media/social web [16] [5]. Browser based attacks can be elaborated into specific vulnerabilities on the following platforms: Firefox, Internet Explorer, PDF, SWF, ActiveX and MS Office.

Moreover, when considering the works of Evans, Kim and research from F-Secure, the following threats emerge: identity theft, spam, hacking, denial-of-service, violation of digital property rights and cyber bullying [4] [13] [6].

Various threats that are critical to Internet Cafés in rural areas were thus identified. These threats should be adequately reflected in the needs assessment to design a cyber security awareness campaign for Internet Cafés in rural areas. In the next section a mapping is given of threats and uses as part of the needs assessment process.

#### 4.1.3 Mapping of Internet uses and threats

In Table 2, a sample mapping is shown of Internet uses to prominent threats. This serves to show the relation between critical threats and their functionality in core Internet uses. The identification of the crucial threats to Internet users in rural areas will be used to determine appropriate topics for the development of awareness material, which is the next step in the application of the NIST framework.

In Table 2 the Internet uses are ticked as columns of the corresponding threats as a means of showing their application. Certain threats were clustered together under a high-level banner to demonstrate that their core underlying functionality could be grouped. For example, malware is the high-level classification for viruses, adware, scareware, spyware, worms, Trojans, password/info stealers, backdoors, downloaders, droppers and rootkits. Browser-based threats were broken down into Firefox, Internet Explorer, PDF, SWF and MS Office. Hacking (exploits) was considered as the high-level category that social engineering, inherent software vulnerabilities and patch management could correspond to.

The legends indicated in Table 2 denote the applicability of the threats to the uses at Internet Cafés. The symbol 'X' denotes "not applicable". An example is that physical harm cannot occur from using an Internet Café to search for information on the Internet. The tick symbol denotes that the threat is applicable to the given use. An example of this scenario is a Web Browser that can be exploited via a vulnerability when using it for entertainment purposes. The symbol 'P' denotes "partial applicability". This is used to indicate that the threat can apply only in certain circumstances. An example is a phishing attack where a user's information can be harvested by searching for information. Some web sites require the user to provide personal details to obtain access to the content. The user can not verify that the web site would adhere to a policy to not share the captured data with external entities.

The various types of malware and browser-based threats, for example, span all the uses of the Internet and therefore a tick is indicated for each of the threats. Similarly, spam is another threat that covers all the Internet uses because a user chatting, using email or when signing up to download music or software has the potential to be spammed. The same principle applies when access to information resources is prevented due to a denial of service (DOS) attack.

Software has inherent flaws that can be exploited in order to take advantage of systems. Software is used in almost every application from email to downloading music and gaming. Thus, it is evident that the threat of inherent software vulnerabilities is applicable across all uses of the Internet. This also implies that patch management would mitigate possible exploitation of the software, preventing interruptions of operations at the Internet Café. Patch management is therefore also applicable to all uses of the Internet as updates are relevant to the various uses of the Internet.

Furthermore, threats that have a psychological perspective are also relevant to users in Internet Cafés in rural areas. Users can divulge information that could assist attackers to physically locate them, entice them to provide more personal information or convince them to perform actions that they would not have done under normal circumstances. Data could be collected during an online chatting session or with the use of social networking sites that record geo-location data posted by the user. This can eventually lead to physical harm if the user is tracked down and attacked based on information collected online. The Internet provides platforms where users can be hurt or embarrassed: text or images could be sent or posted to intentionally spread false and negative information. The viral nature of the Internet will spread the information beyond the control of the person who posted the information. The use of the Internet for communication and entertainment is important components for people to stay in touch. However, care should be taken in what data people share on these platforms. Threats like cyber bullying, physical harm and the spreading of negative information are mainly relevant to the use categories of entertainment and communications as the mechanisms of chatting computer games, signing up for music or software for one's own amusement, social networks and email fall into these categories.

Moreover, techniques like social engineering also rely on influence to lure or trick users into performing an action by creating a relationship and then taking advantage of the trust created to manipulate the user. The user can be lured into unintentionally providing more personal information by visiting a phishing site or becoming the victim of a scam. The attackers could use the trust already established to trick the user into making payments for products or services with the intention not to provide the actual services. The faceless characteristic of the Internet creates these devious opportunities. Data collected during a phishing attack can be used to impersonate a user. Identity theft provides attackers with avenues to conduct financial transactions without establishing the validity of the credentials of the person. Phishing, identity theft, online scams and fraud are devised by the user's participating in a two way communication and providing data that can be stored and later used by attackers. Phishing and online scams are mainly relevant to financial, business and communication

uses of the Internet. Identity theft has partial applicability to business and entertainment uses, but is still applicable to financial and communication uses.

In addition, the Internet also poses various threats that may have legal implications. Internet Cafés users can download copyrighted software, music, books or content that infringes on digital property rights and these offences may be punishable. Legal and regulated gambling sites may not provide sufficient winning margins which means users may search for unregulated gambling sites that provide higher winning margins. These sites are created for the black market where cyber laws may not be adhered to. Prosecution of unlawful action is not always possible, for example in the 419 scams users were tricked to deposit large amounts of money and the operators of the sites disappeared without providing a service. Online scams and illegal online gambling are mainly applicable to the business and financial uses of the Internet.

**Table 2: Mapping of Internet Uses to Threats**

Use/Threat	Info	Entertainment	Financial	Business	Communications
Spam	✓	✓	✓	✓	✓
DOS	✓	✓	✓	✓	✓
Phishing	P	P	✓	✓	✓
Violation of digital property rights	✓	✓	X	✓	P
<i>Malware</i>					
Virus	✓	✓	✓	✓	✓
Adware	✓	✓	✓	✓	✓
Scareware	✓	✓	✓	✓	✓
Spyware	✓	✓	✓	✓	✓
Worms	✓	✓	✓	✓	✓
Trojans	✓	✓	✓	✓	✓
Password/Info stealer	✓	✓	✓	✓	✓
Backdoor	✓	✓	✓	✓	✓
Downloader	✓	✓	✓	✓	✓
Dropper	✓	✓	✓	✓	✓
Rootkit	✓	✓	✓	✓	✓
<i>Browser Based</i>					
Firefox	✓	✓	✓	✓	✓
IE	✓	✓	✓	✓	✓
PDF	✓	✓	✓	✓	✓
SWF	✓	✓	✓	✓	✓
ActiveX	✓	✓	✓	✓	✓
Opera	✓	✓	✓	✓	✓
MS Office	✓	✓	✓	✓	✓
<i>Hacking(Exploit)</i>					
Social engineering	X	✓	✓	✓	✓

Inherent software vulnerabilities	✓	✓	✓	✓	✓
Patch management	✓	✓	✓	✓	✓
Online scams and fraud	✓	P	✓	✓	✓
Physical harm	X	✓	X	X	✓
Cyber bullying	X	✓	X	X	✓
Spreading false or negative information	X	✓	X	X	✓
Illegal online gambling	X	X	✓	✓	P
Identity Theft	X	P	✓	P	✓

The main aim of mapping threats to the Internet uses is to identify and prioritise critical topics that are essential for the cyber awareness campaign. The mapping provides a method of ascertaining which threats are pertinent to users of Internet Cafés in rural areas. This output will feed into the next step of applying the NIST framework: Developing Awareness Material.

## 4.2 Develop Awareness Material

To develop the awareness material, information gathered from the needs assessment will be utilised to select awareness topics. The topics can then be researched in order to develop the content.

The content of an awareness program is determined by the needs that have been identified. The identification process described in Section 4.1.3 produced a list of potential threats that can be encountered at Internet Cafés. The different threats can be studied to determine those that will have the highest impact on the users at Internet Cafés. A discussion follows on the relevance of certain threats to users of Internet Cafés in rural areas. The discussion commences with the elimination of certain threats by explaining why they are not priority topics of awareness creation for users of Internet Cafés in rural areas. The discussion then moves on to relevant threats for which awareness should be created.

### 4.2.1 Motivation for elimination of threats

While spam can be encountered with all the uses identified at Internet Cafés, the mitigation of these attacks is not part of the knowledge and skill set of an average Internet Café user. These users usually will connect to their email using a web browser. Spam filtering is part of the services provided by the email providers and the user has no control over this. While the users can reactively create rules to discard certain spam messages, it is the service provider who is required to provide protection at a higher level. The user also has no control over a denial of service attack. These attacks occur when attacker utilises services to prevent users accessing resources on the Internet. The violation of digital property rights is not a high priority threat as not all Internet Cafés provide the service of creating duplicate copies of digital content with the use of burners. Extra hardware would be required which will have a financial impact and the owners of these establishments could be liable for the violation of digital property rights.

Users make use of browsers to access the Internet at Internet Cafés. Browsers are software with inherent vulnerabilities which requires updates or patches to provide security to the users. The browsers are utilized third party software to provide additional functionality. For example a web browser can use Acrobat Reader to open a PDF file in the browser. This will allow the user to read the file. Ensuring that the browser is fully updated with the latest patches, does not ensure that the third party software is updated. Due to the technical nature, this threat should be mitigated by the technical team of the establishment.

Malware is a prevalent threat which affects all the uses at an Internet Café. The different types of malware as described in Table 2 can be executed on a system by a user. Users can be lured into performing these actions with or without their knowledge. Certain malware, for example, downloaders, droppers and Trojans, can be installed on a system by simply visiting a web site with a vulnerable web browser. The other malware can be installed by users executing malicious software. For example,

viruses or worms could use the network to identify vulnerabilities on systems on the network and infect the systems. Malware infections can be mitigated by using software that provides protection on these levels. In the context of the Internet Café, the establishment should ensure that these protection tools are available and updated.

#### **4.2.2 Motivation for applicability of certain threats**

The remaining threats: phishing, social engineering, scams, cyber bullying, physical harm, spreading false or negative information, illegal online gambling and identity theft are recommended topics for security awareness programs for Internet Café environments. Users can decide on the actions they perform and no technical skills are required to mitigate these threats.

The purpose of an awareness program is to provide users with the knowledge to identify and mitigate these threats. Using casual chains it is possible to identify that social networking sites and email are uses of the Internet where these threats are predominant. The potential exploitation when using the Internet for email and social networking, are applicable topics for awareness creation to most Internet Café users as information that is disclosed can be used to attack users and perform other attacks on the infrastructure of the establishment. For example, personal information could be used to spread false information or used in a cyber bully attack or collect data to perform a social engineering attack. Localisation information could be used to determine the physical location of a user at a specific time which could create an opportunity for physical harm.

Attackers could implement influence techniques to trick users into performing actions or participating in events that affects the users negatively. Users at Internet Cafés are prime targets for emails that can be used to promote illegal online gambling, being lured into scams and phishing sites. For example, a user can receive an email from an illegitimate financial establishment. The content of the email will look authentic. An uninformed user will implicitly trust the email and comply with the request in the email by clicking on the link and providing data requested. A user who is aware of phishing attacks would have looked at the source of the email, the legitimacy of the address of the web site and be aware that no financial establishment would request authentication information in an email. Furthermore, data collected from phishing sites can be used for identity theft.

Therefore, based on the previous discussion, the issues identified as most critical for which material should be developed for an awareness campaign for users in Internet Cafés in rural areas are: phishing, social engineering, scams, cyber bullying, physical harm, spreading false or negative information and illegal online gambling. The next step addresses the implementation of the awareness program.

#### **4.3 Implement the Awareness Program**

Awareness material can be delivered to users via Interactive video training (IVT), web-based training, non-web computer-based training, or instructor-led training.

The nature of an Internet Café influences the method used to deliver the awareness program. In Section 3.3 the different types of delivery methods were discussed. They include formal training sessions, strategic placement of awareness messages, passive computer-based, web-based and interactive computer based training. In this application of the NIST framework, the placement of awareness messages and passive computer based training will be more effective in Internet Cafés. The users will not be distracted from the initial intention of using the services at the Internet Café. Computer based training modules could be installed on the computers which will allow the users to use it when required. Formal training session and discussion groups are not suited for an Internet Café, as these types of delivery methods will impede on the users' need to use the Internet services provided.

After studying the various mediums for delivering material, a selection will be chosen depending on the resources and complexity of the message. In this case study, the use of posters, screen savers, a message of the day, or a pop-up message on the computer can be chosen to deliver content to the Internet user.

The topic chosen for awareness creation in this example, Phishing, can be explained to users as emails sent with malformed URLs imitating legitimate banking, financial or shopping services. This message can be designed to appear in a pop-up message or screen saver.

#### 4.4 Post-Implementation

Thereafter, the awareness campaign can be evaluated to determine whether it was effective in educating users. Feedback and evaluation can be carried out through;

- Interviews to determine awareness levels.
- Questionnaires to determine awareness levels.
- Analysis of online behaviour to determine if phishing sites were visited.

#### 5. Conclusions

This paper discusses the use of the NIST framework to design cyber security awareness programs for Internet Café users in rural areas. The authors motivate that there exists a dire need for security awareness among Internet Café users, and especially Internet Café users in rural African areas. Africa has the lowest percentage of Internet users in the world and it has poor telecommunication infrastructure. These factors combined with poverty, especially in rural areas, lead to Internet Café being the only access point for a majority of rural Africans. These Internet users are often unemployed and will thus not have access to security awareness programs delivered by larger businesses. Internet Cafés provide the means for the less fortunate to empower themselves by accessing online services and acquire knowledge from the content available on the Internet. Unfortunately accessing the Internet is a double-edged sword and with all the advantages of the Internet, also comes the dangers of the cyber world to the uninformed user.

Some frameworks exist to create security awareness programs to address the dangers that are present at these establishments. The NIST framework consists of sequential steps that identify a need through the collection of information and the subsequent development and delivery of the content which address the inadequacy of security awareness demonstrated by users and owners at Internet Cafés. The framework also provides a mechanism to evaluate the success of the security awareness program. However, this paper addresses the feasibility of the framework to identify content specific for Internet Cafés. The application of the framework in this paper identifies the different usages of Internet Cafés and the different threats that can be encountered at these establishments. Furthermore, an analysis of the identified uses and threats provide a summary of security related topics that are specific to Internet Cafés. Some of these topics include, but are not limited to, Phishing, social networking, spam, malware, identity theft and browser based attacks. The Internet is an ever-changing landscape and with the technology evolving so do the threats. Internet users should be empowered to be able to mitigate these threats. Users can access the Internet from different access points. This paper addressed a process of using a framework to create a security awareness program to address threats at one of these access points namely the Internet Café.

#### References

- [1] D. Anselmi and R. Boscovich , "Microsoft Security Intelligence Report," Microsoft, Tech. Rep. 9, pp. 1-76, 2010.
- [2] Cyber Internet Café , "Internet Café History", Accessed 20110307, Available online at <http://www.cyber-internet-cafe.com/internet-cafe-history.html>.
- [3] Chanel De Bruyn , "EASSy undersea cable launched, capacity almost trebled", Engineering News, Accessed 20110303, Available online at <http://www.engineeringnews.co.za/article/eassy-undersea-cable-launched-capacity-almost-trebled-2010-08-05>.
- [4] J. Evans, "A Brief Analysis of the Cyber Security Threat," Hacking9, vol. 5, issue. 11/2010(36), pp. 46-49, 2010.
- [5] J. Evans, "The Social Web Threat," Hacking9, vol. 6, issue. 01/2011(37), pp. 46-49, 2011.
- [6] F-Secure , "Threat Types", F-Secure, Accessed 20110304, Available online at [http://www.f-secure.com/en\\_EMEA-Labs/virus-encyclopedia/articles/classification/threat-types.html](http://www.f-secure.com/en_EMEA-Labs/virus-encyclopedia/articles/classification/threat-types.html).

- [7] B. Furuholt and S. Kristiansen, "A Rural-Urban Divide? Regional Aspects of Internet Use in Tanzania", *Proceedings of the 9th International Conference on Social Implications of Computers in Developing Countries*, 2007.
- [8] B. Furuholt and S. Kristiansen, "Internet Cafes in Asia and Africa - Venues for Education and Learning?", *Journal of Computing*, vol. 3, 2007.
- [9] B. Furuholt, S. Kristiansen and F. Wahid, "Gaming or gaining? Comparing the use of Internet cafés in Indonesia and Tanzania", *The International Information & Library Review*, vol. 40, pp. 129-139, 6 2008.
- [10] J. Hobbs and T. Bristow, "Communal computing and shared spaces of usage: a study of Internet cafes in developing contexts", *ASIS&T IA Summit, Las Vegas, March*, pp. 22–26, 2007.
- [11] N. Hyde-Clark, "The Urban Digital Divide: A Comparative Analysis of Internet cafes in Johannesburg", *Review of African Political Economy*, vol. 33, 2006.
- [12] Internetworldstats , "Internet Usage Statistics for Africa", Accessed 20101111, Available online at <http://www.internetworldstats.com/stats1.htm>.
- [13] W. Kim, O. Jeong, C. Kim and J. So, "The dark side of the Internet: Attacks, costs and responses", *Information Systems*, Elsevier2010.
- [14] E. Kritzinger and S.H. von Solms, "Cyber Security for home users: A New Way of Protection through Awareness Enforcement", *Computers & Security*, vol. 29, pp. 840-847, November Elsevier2010.
- [15] R. Manning, "Phishing Activity Trends Report," Anti Phishing Work Group, Tech. Rep. 2nd Quarter, 2010.
- [16] A. Menon and M.G. Gabriely , "State of the Internet 2010: A Report on the Ever Changing Threat Landscape," CA Technologies, 2010.
- [17] M. Milicevic , "Cyberspace and globalization", Paper presented at CSIR Conference Centre, Pretoria, South Africa, Accessed 20110307, Available online at [http://www.ais.up.ac.za/digi/docs/milicevic\\_paper.pdf](http://www.ais.up.ac.za/digi/docs/milicevic_paper.pdf).
- [18] S. Molawa, "The First and third World in Africa: Knowledge Access, Challenges and Current Technological Innovations", *Proceedings of the 1st International Conference on African Digital Libraries and Archives*, 2009.
- [19] S.M. Mutula, "Cyber Cafe Industry in Africa", *Journal of Information Science*, vol. 29, 2003.
- [20] P.G. Mwesige, "Cyber elites: a survey of Internet Café users in Uganda", *Telematics and Informatics*, vol. 21, pp. 83-101, 2 2004.
- [21] J. Otieno , "Africa: Low Internet Usage the Bane of Africa's Digital Media", Accessed 201011/18, Available online at <http://allafrica.com/stories/201003190904.html>.
- [22] M. Polychronakis, P. Mavrommatis and N. Provos, "Ghost turns zombie: exploring the life cycle of web-based malware", in *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, pp. 1-8, 2008.
- [23] Seacom , "Seacom goes live", SEASCOM, Accessed 20110303, Available online at [http://www.seacom.mu/news/news\\_details.asp?iID=100](http://www.seacom.mu/news/news_details.asp?iID=100).
- [24] TelecomPaper , "Teams cable launches in Kenya", Telecompaper, Accessed 201103/03, Available online at <http://www.telecompaper.com/news/teams-cable-launches-in-kenya>.
- [25] A. Twinomugisha , "Why Are African Internet Access Prices Still High?", Accessed 20100209, Available online at <http://www.africabusinesssource.com/experts/why-are-african-internet-access-prices-still-high/>.

[26] M. Wilson and J. Hash, "Building an information technology security awareness and training program", *NIST Special Publication*, vol. 800, pp. 50, 2003.



# Design of cyber security awareness game utilizing a social media framework

**WA Labuschagne**  
UNISA  
Pretoria, South Africa  
wlabuschagne@csir.co.za

**I Burke**  
CSIR  
Pretoria, South Africa  
Iburke@csir.co.za

**N Veerasamy**  
CSIR  
Pretoria, South Africa  
nveerasamy @csir.co.za

**MM Eloff**  
UNISA  
Pretoria, South Africa  
eloffmm@unisa.co.za

*Abstract*— Social networking sites are a popular medium of interaction and communication. Social networking sites provide the ability to run applications and games to test users' knowledge. The popularity of social networks makes it an ideal tool through which awareness can be created on existing and emerging security threats. This paper proposes an interactive game hosted by social networking sites with the purpose of creating awareness on information security threats and vulnerabilities. The game applies principles of good game design which includes: the decisions over hypermedia, multimedia and hypertext to achieve perception, comprehension or projection, comprehensive database of questions, weighted system, use of practical data, automation, dynamcis, effort and user acceptance. The aim of the paper is show the effectiveness of using a virtual tool in cyber awareness creation. This paper will thus deal with the proposal of an interactive web-based game which informs and then tests users about potential security threats and vulnerabilities.

*Keywords*- application, awareness, security, social networking, threat, vulnerability

## I. INTRODUCTION

It is becoming increasingly important for all users, and not just technical staff, to be aware of safe cyber practices. Eminagaoglu et al. [1] state that not only technical security training of IT staff, but also information security awareness training and other awareness campaigns have become a "must" for everyone. Many users are ignorant of the range of threats spanning cyber space and the Internet. By using cyber security campaigns, awareness can be created on current threats, as well as educate users on best practices to identify and handle threats. Another prime target for awareness creation is universities. According to Rezgui & Marks [2], a number of universities now recommend providing security awareness training and education components for students and staff, and emphasize that everyone needs to be aware of up-to-date IT threats so they can apply the security lessons in the most effective way. Home users could also benefit from cyber security awareness

campaigns that warn them of the latest threats or provide useful tips on safe internet surfing. Kritzinger & von Solms, [3] state the vulnerability of personal Internet users is due to the fact that they lack the information security knowledge to understand and protect their PC and therefore also their personal information.

One way of creating awareness is by utilizing popular mediums such as social networking sites. Social networking sites ideally serve the purpose of awareness creation as users are keen to try out new games and applications. Various marketing and educational schemes can benefit from the popularity and reach of social networking sites. Social networking sites have the ability to post results from quizzes and games allowing users to compare their scores. This approach could be utilized in order to create a game to measure and increase users' awareness on cyber security. This paper therefore proposes the design of virtual game with the goal of improving cyber awareness. The remainder of the paper is structured as follows: Section II provides a motivation for the game and Section III introduces the requirements for the game design. Section IV provides a brief overview of similar games aimed at increasing user security awareness Section V, explains the operation of the proposed game and the paper is concluded in Section VI.

## II. MOTIVATION FOR GAME DESIGN

### A. Directed Communication

Albrechtsen & Hovden [4] mention forms of one-directional communication such as pamphlets, emails, intranet pages, screen savers, posters, mouse pads, pens, games, formal presentations and training sessions which are largely aimed at transferring information from an authority to the target population. Furthermore, they wish to emphasise the importance of employee feedback and participation as it can greatly improve the employees' information security awareness and behaviour. This argument shows that success of employees

retaining the security awareness knowledge is increased when users actively engage in the process and are not merely subject to one-sided instruction and distribution of facts. Rezgui & Marks [2] argue that it is paramount to enforce awareness and training as human errors are rated as among the top security threats. When considering the financial implications of a single case of abuse, the necessity of ensuring all users are aware of information security threats becomes obvious. Furthermore, Eminagaoglu et al. [1] show in a case study show that awareness training and related campaigns can have a positive effect on reducing security threats. In their study, the results showed that weak password usage was significantly decreased and users continually improved their awareness and complied with policies after under-going a security awareness training course. In addition, Dodge Jr. conducted a phishing email exercise by generating a phishing email with embedded links, as well requests for sensitive information [5]. After carrying out the experiment at a military academy the amount of students falling victim to the scam was measured. Thereafter training was given with the intent of reducing students' propensity of falling victim. By providing the awareness programme, the number of students at the university falling victim to the phishing exercise dropped each year which showed that they were now able to recognize potential scams. These results show that awareness levels can be increased through interactive content. This also indicates that the medium through which awareness material is provided also plays a significant role.

### B. Information Richness

Shaw, Chen, Harris and Huang [6] argue that the Web is an ideal tool to deliver security awareness as it is able to handle the needs of multimedia (audio, video and animation) to reflect real scenarios of information risks. This also raises the issue that information richness of different forms of multimedia can affect the effectiveness of online security awareness programs. Furthermore, they discuss three media that are pertinent to the influence of information richness on the effectiveness of online security awareness programmes. These are [6] :

- **Hypermedia:** interactive medium that consists of graphics, audio, video, plaintext and hyperlinks which makes it the richest medium of the three. Concepts can be arranged visually and not sequentially to help users understand critical concepts and their interrelationships.
- **Multimedia:** combines text, image, sound, music, animation, video and virtual reality but must be accessed in a linear sequence.
- **Hypertext:** does not incorporate feedback, language variety, multiple signals or personal focus.

Through their study on a selection of security inexperienced users, Shaw et al. [6] were able to deduce:

- That hypermedia and multimedia were more effective in enhancing users comprehension and projection ability of security awareness,

- Hypertext-based training was more effective than multimedia in enhancing users' perceptions of security risks.
- Perception refers to a basic awareness of the security topic.
- Comprehension entails understanding the technical operation of the exploit.
- Projection would involve predicting a future route to follow.

These results provide important insight when designing a game for security awareness creation. The richness of the media, together with the aimed level of awareness are important decisions in the design of a game to create security awareness. These decisions were considered in the design of the proposed security awareness game.

After having identified the necessity of creating security awareness and studying the mediums of content distribution, the discussion moves on to the compilation of essential requirements that will form the basis of the proposed game design.

### III. REQUIREMENTS

In the previous section, the effect that media richness plays in affecting the awareness levels created were discussed. A decision on media richness is thus required when designing web-based game for awareness creation. In addition, other requirements for a web-based security awareness game should also be considered. The design of the game consists of different components, which should be taken into consideration to ensure that the objective of the platform is achieved, as well as to ensure that the users will be actively involved in the act of playing the security awareness game. Kruger and Kearner [7], Hsu and Lu [8], Shin and Shin [9], Johnston [10] and Priebatsch [11] proposed components that should be considered in the development of successful security awareness games using social networking sites. This section summarises some key requirements that fed into the design of the security awareness game for security awareness creation. These requirements include, but are not limited to, the following:

1) **A comprehensive database of questions should exist** – The nature of the proposed game would require a database of questions. This is used to determine the current knowledge level of the users and also be used as a critical game component. Quality time ought to be spent obtaining the right input for the game. A large set of questions also allows for a random set to be selected each time. An extensive database with questions should prevent the application from presenting the same questions to the user. The question database should ensure that the topic is sufficiently covered and that the topics cover the subject matter in depth while the range of topics are extensive.

2) **Weighting of the questions** – It is recommended to assign higher weights to questions that are more challenging. This would allow the game to progressively become more difficult as the users knowledge increases. In addition, the use

of weights would create levels in the game which could be used to determine the current security awareness of the user.

3) **The use of practical data** – The data encapsulated in the questions should reflect real life scenarios that users could easily identify with. User participating in the game should be able to apply the knowledge acquired during the game play in their current environment. The relevance of the data should be applicable and disseminated into easy interpretable knowledge fragments. For example the user playing the game on the social networking site would not have the technical knowledge of a server administrator. Hence the questions should not cover server administration security threats. It will be more feasible to develop the question bank that covers security threats that are encountered by every day users. Commtouch [12] reported on the trends of Internet threats in the first quarter of 2011. These trends provide a list of threats that users need to be aware of and could be reflected in the content of the game play. These topics could be changed into the questions and placed into the different question topics that covers each security threat.

4) **Tool should be automated** – The mechanism used to conduct the security awareness program should be designed to function without the intervention and supervision of humans. All the required calculations should be computed by the system and guide the users through the entirety of the application. The removal of the human component from the system suggests that multiple users from numerous locations can play the game simultaneously. This is an important component since social networking sites are Internet based which allows multiple users to interact with the game.

5) **Game dynamics** – All game design involves different gaming dynamics which incite users to come back and play again. Priebatsch [11] discussed four game dynamics that should be present in on-line games, namely Appointment, Influence and Status, Progression and Communal discovery dynamics. The Appointment dynamic ensures that users return to the game due to a temporal event which subconsciously commits the user to returning to play the game over time. The Influence and Status dynamic makes use of symbols for example badges representing status to compete with other peers. The Progression dynamic provides feedback to the user of progress made. The Communal discovery dynamic allows users to collaborate with other users to solve complex problems.

6) **Easy accessible** – The game developed should provide users easy access to the required resources. Resources that are located on a personal computer at home or located within a private internal network are not easily accessible. The Internet architecture is developed to provide mechanisms for users to access resources easily. For example, a user requires an Internet connection, computer with web browser and the address of the resource for access. Web sites are easily accessible and thus can cater ideally for the requirement of accessibility. The advances in personal computers, laptops, mobile devices allows users to access these web sites

7) **Effortless** – Computer/Graphical Interfaces provide users a mechanism to interact with technology, this would also imply that the interface determines how the user will experience this interaction. Human Computer Interfaces (HCI) is defined by Johnston, Eloff and Labuschagne [10] as: "HCI deals with the interaction between one or more humans and one or more computers." A list of ten critical factors, listed below, was developed by Nielsen [13]. These factors provides the users with an experience which build trust with the application, increase productivity and reduces erroneous use, which frustrates the user . The development of the interface that will be used by the users to interact with the game will incorporate these factors in the design. Social networking sites use these factors as part of its design in order to ensure ease of use. The factors from Nielsen are:

- **Visibility of system status:** The system should always keep users informed about what is going on, through appropriate feedback within reasonable time
- **Match between system and the real world:** The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.
- **User control and freedom:** Users often choose system functions by accident and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support functions of undo and redo.
- **Consistency and standards:** Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.
- **Error prevention:** Even more beneficial than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
- **Help users recognize, diagnose, and recover from errors:** Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
- **Recognition rather than recall:** Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
- **Flexibility and efficiency of use:** Accelerators -- unseen by the novice user -- may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.

- **Aesthetic and minimalist design:** Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
- **Help and documentation:** Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

8) **Acceptance by the user** – The longevity of the game is determined by numerous factors. The game requires users to participate by playing with the designed tool. Also, it is critical for users to return to the game. The game would require factors that would entice users to return. The user interface as discussed earlier is one of the required factors. The Technology Acceptance Model (TAM) was originally proposed by Davis [14]. Furthermore, Moon [15] states that TAM provides determinants of individual adoption and can explain and predict the individual's acceptance of Information Technology (IT). Moreover, Moon states: "This model illustrates that the social behaviour is motivated by the attitude towards carrying out that behaviour, a function of one's beliefs about the outcome of the performing that behaviour and an evaluation of the value of each of those outcomes". Fig 1 illustrates the different determinants of TAM as originally specified by Davis [14].

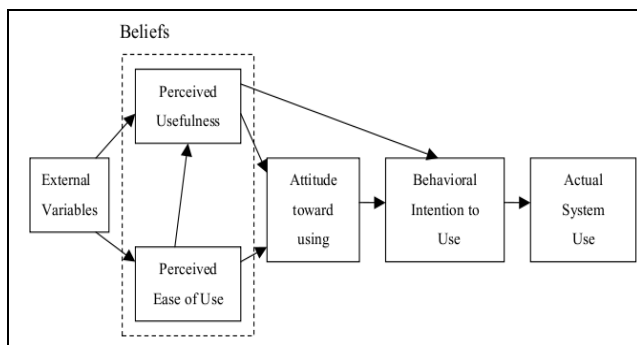


Figure 1. TAM Model

Users encountering new technology for the first time experience two determinants. The user questions the usefulness and the ease of use of the new technology. Perceived Usefulness (PU) and Perceived Ease of Use (PE) affect the belief of a user which influences the attitude towards using the technology, also affecting the behaviour to finally use the system [16]. The TAM has been extended by Hsu & Lu [8] to address on-line games (See Fig 2). Two additional determinants has been added: Social influences and Flow experience. Social influences has been identified to shape user behaviour through social norms demonstrated by other groups.

People tend to look upon other's behaviour when faced with a situation whereby they do not know how to react [17]. Csikszentmihalyi [18] defined the concept of flow as "the holistic experience that people feel when they act with total involvement". This definition suggests that flow consists of four components—control, attention, curiosity, and intrinsic interest. The number of social networking sites have exploded in recent times providing platforms whereby users could create content, build relationships and also participate in entertainment such as playing games. Shin & Shin [9] identified the need to adapt the TAM to accommodate social networking sites with the addition of the following determinants: Perceived Playfulness (PP) and Perceived Security (PS). These two determinants addresses the level of curiosity during an interaction with technology and the security concerns that have been raised with use of social networking sites. They found that PP was related to PE and PU. Therefore the determinants: PE, PU, PS, PP and flow are important factors that need to be reflected in the design of a game utilising social networking sites.

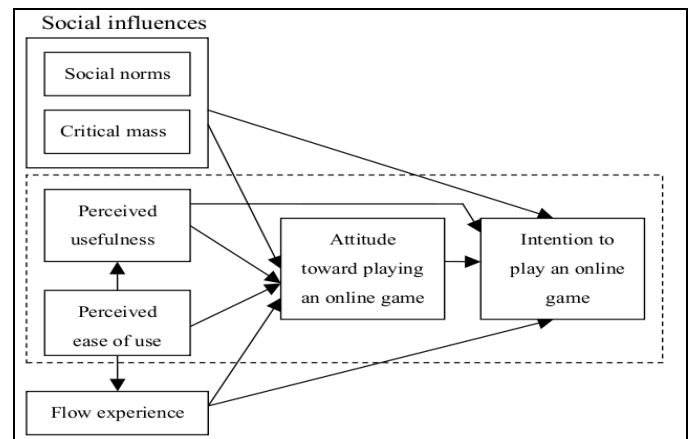


Figure 2. Extended TAM Model

#### IV. SECURITY AWARENESS GAMES

Cone [19] found that video games can be effective in basic information security training programs. His study focused on a game developed by the Center for Information Systems Security Studies and Research (CISR) for the Department of Defense of the United States of America called CyberCiege [20]. This game is a highly extensible game for teaching information assurance concepts and runs on a standalone computer system. The game is based on different scenarios whereby the user needs to take certain actions to learn about threats and acquire the knowledge to prevent and mitigate the threats. The scenarios include, but not limited to the following topics: Stopping Worms, Life with Macros, Identity Theft, Passwords, Physical Security, Patches, Filters, Encrypt Link and Identity management. The users learn about a topic through the use of the game and experience obtained through the approach of problem solving and critical thinking. Another game, from the USA Department of Defense called CyberProtect [21], provides users with an interactive security

experience. Screenshots from the CyberProtect game are shown in Fig 3 and Fig 4.

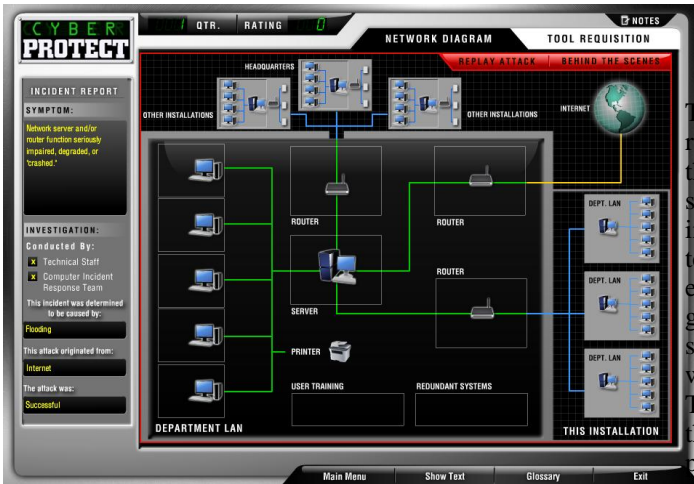


Figure 3. CyberProtect

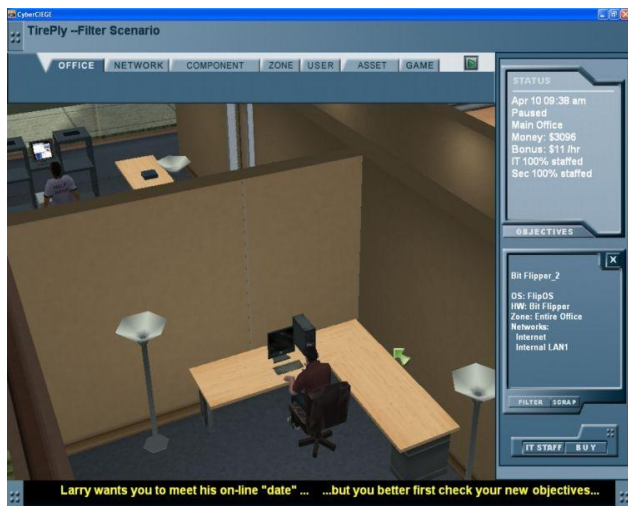


Figure 4. Cyberprotect

This game is an on-line game but does not use a social networking site as the delivery platform. This game is also more focused on securing a network and all the threats that are in the network domain. This game is designed for a specific audience that has background knowledge in networking technology and implementing strategies to secure the network.

Social networking sites have numerous successful games for example Farmville, Mafia Wars, Farm Town and Petville. The success of these games could attribute to the design of future games.

Social networking sites provide an accessible portal through which to gain access to a networking site that already have an extensive user base. There is thus a gap for games using social networking sites and due to this requirement, the proposed design for such a game is given in the next section. There is thus a gap to use social networking sites to play games that promotes cyber security awareness. .

Using all these identified requirements, a proposed design for a security awareness game is given in the next section.

## V. DESIGN OF GAME

The basic outline of the game is presented in this section. The design of the game takes into consideration the various requirements discussed in the previous sections. The design of the game is given in the conceptual prototype explained in this section. Principles that the requirements capture are incorporated in the conceptual prototype that has been partially tested but not deployed in the social networking site environment as yet. Fig 5 shows the high-level design of the game. To commence the game, the user logs on the login screen. Thereafter the user is presented with the topic tree which shows topics graphically and in a listed format. The Topic Tree page also displays the most recent achievement by the user. Once the user has selected a topic (for example password security), he/she is provided with the option to choose a video, slide show or quiz. The slides and videos are used for education purposes while the quiz feature is used to determine the knowledge that the user currently has or has acquired. The other options for the user include viewing achievements on the My Profile Page or viewing the current leader board. In general, the user has the ability to log-out which returns the game to the login screen once again. The dashed lines indicated the interlinking between the web pages. The arrowheads on the dashed lines show the navigational direction of the pages. The arrows show the functional flow of the game from login, to topic selection, proceeding to either learning or testing and thereafter viewing of individual achievements or the leader board.

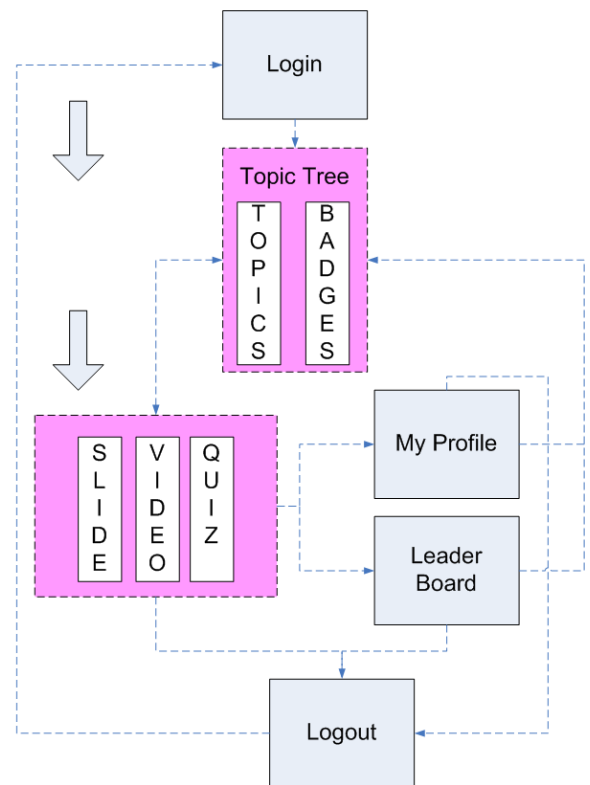


Figure 5. High-level design of game

Screenshots from the conceptual prototype are now provided to show the functional flow explained in the high-level design diagram (in Fig 5).

The overall objective of the project is to primarily promote perception and thereafter comprehension. To achieve this, the findings given in Section II B stipulate that hypertext and multimedia would be ideal. Therefore, the game aims to incorporate components of multi-media and hypertext in order to present an inviting and engaging forum for users to interact with (see Fig 6 and Fig 7). In Fig 6, users may use the hyperlinks on the left or the interactive hotspots to select a security awareness topic. In each topic view, Fig 6, users can choose to view tutorial material related to the topic or attempt answering a quiz related to the topic.

Fig 6 also shows the weighting requirement. The layering of subject matter as described by Khan [22] addresses the

requirement of using a weighted method to incorporate the difficulty of content. Each level represents a more complex level of topics. In order for the user to advance to more advanced topics, a user is required to ‘unlock’ the next level. Users need to answer ten consecutive questions correctly on the preceding level. Questions are chosen at random from the pool of compiled questions for each level. This shows the compliance to the requirement of having a comprehensive database of questions. The questions have been constructed using practical knowledge (see Fig 8). For example Fig. 8 illustrates the testing of a user’s knowledge of sensible passwords, which take into consideration complexity and the possibility of remembrance. The example questions also reflect practical mathematical probabilities of guessing or determining passwords. With these statistics users can understand at a basic level the ease of password cracking that uses dictionary words or plain obfuscation.

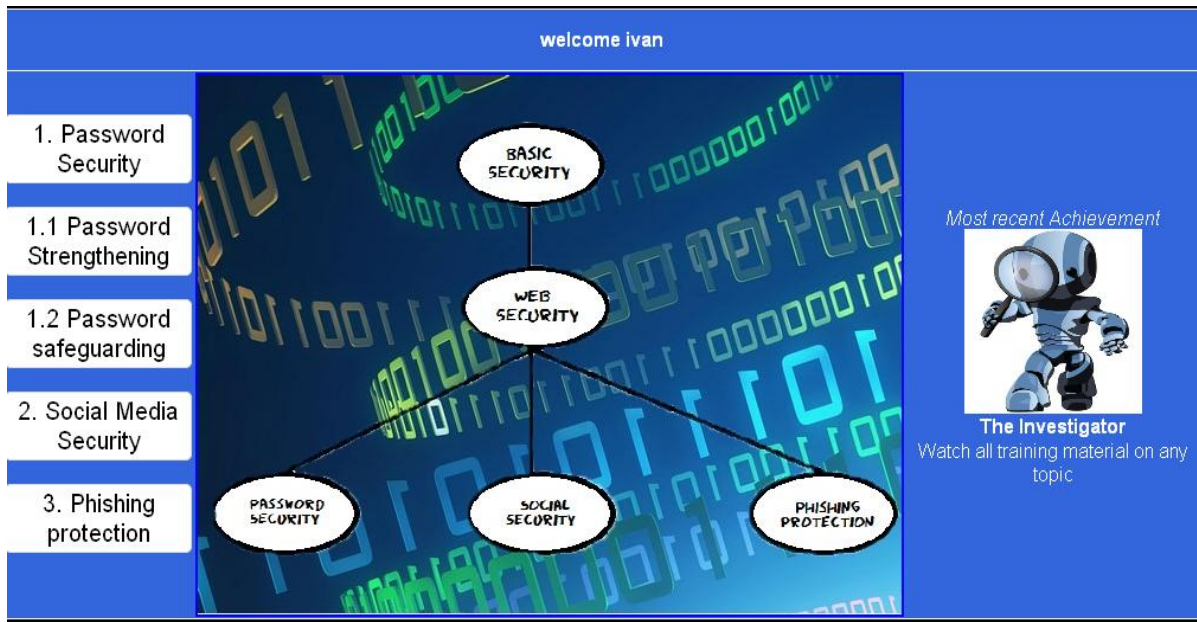


Figure 6. High-level view of game

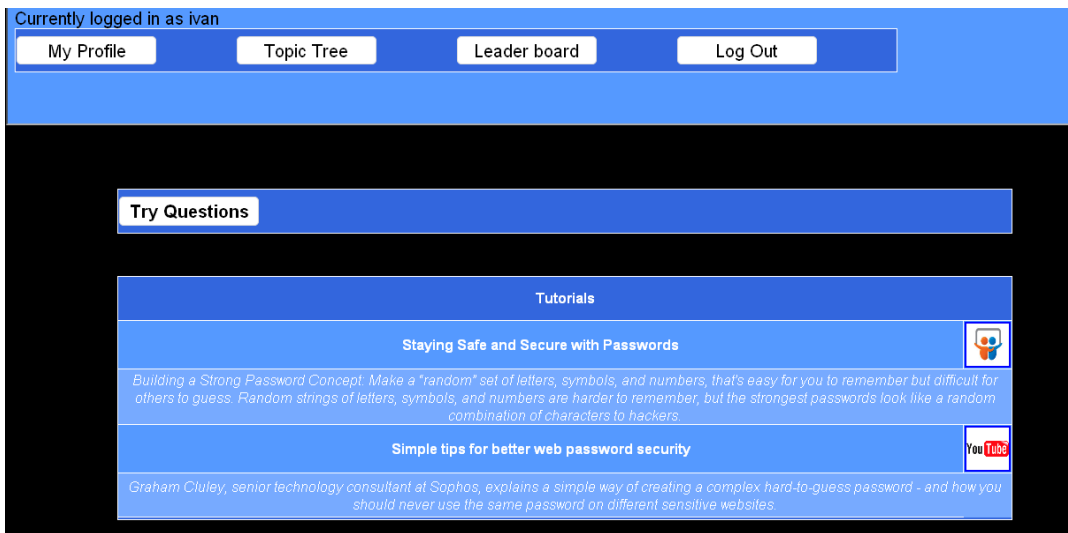


Figure 7. Mix of hypertext and multimedia

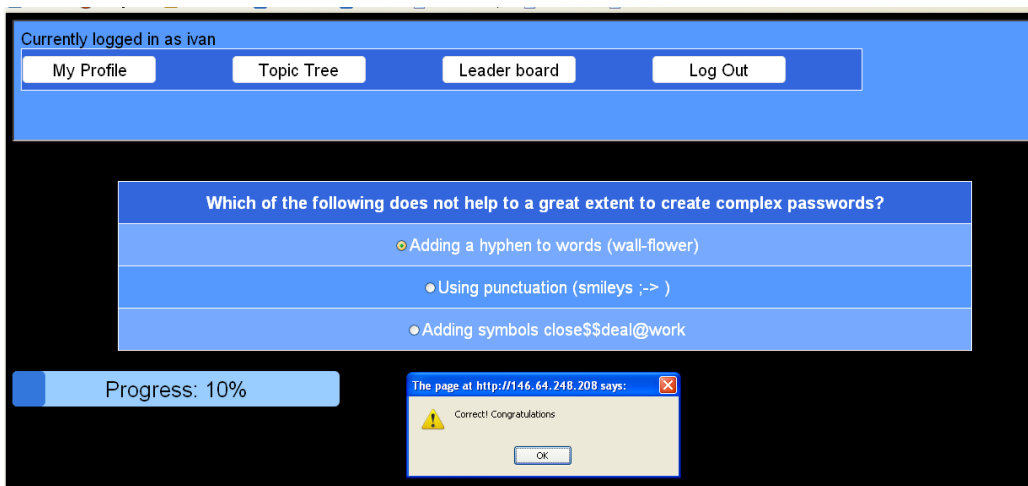


Figure 8. Sample question and status

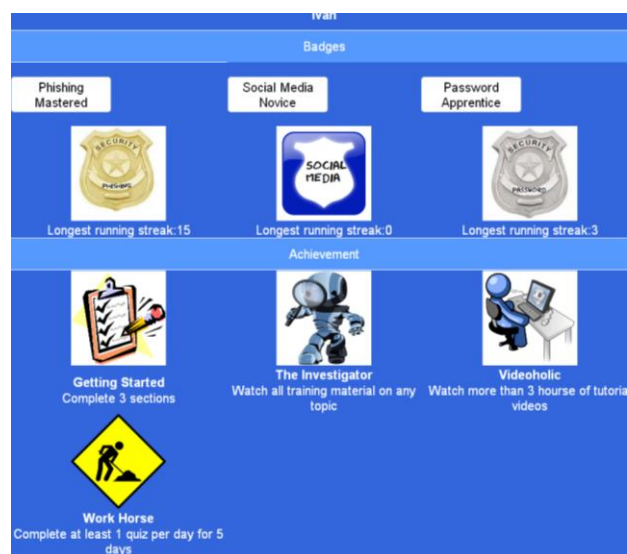


Figure 9. Badge and achievements



The online-game application is automated and does not require human intervention to operate. The game has notifications listing recent achievements. Badges can be awarded to indicate a run of correctly answered questions (see Fig 9). This achievement system promotes return visits as users attempt to attain better scores. For ease of access, the game has been designed to be easily linked to social networking site APIs. Thus, the application can appear as a link on Facebook and users can play the game. Users have the ability to view their friends' scores and thus their friend's progression with the subject matter.

With regards to an effortless interface, the tool directly applies some of the necessary criteria explained by Nielsen [13]. In particular, the system has hyperlinks and status bars to indicate to the users their current location and status. Furthermore, the system has been designed to minimize errors by using hyperlinks for easy navigation and capturing user input through selection controls. Users do not have to recall their current position in the system but can use the controls to identify the desired location. In addition, the interface has been designed with a pleasing aesthetic design, using the theme of cyberspace and security. Relevant information is displayed to ensure that the user understands the instructions and maintains navigational control.

A user's profile displays the badges and achievements attained by the user. The badge and achievement system encourage users to try and attain better scores and complete more sections. By using a social networking application to run the game, users can view their friends' activity and this would also encourage repeat use. In this way, by placing the game in a popular medium such as social networks, the appeal of the game is strengthened and this also promotes user acceptance.

The game has been designed with ease of use and usefulness in mind. Minimalist and intuitive controls, as well as questions providing practical advice form part of the game. Furthermore, since the tool can be linked to social network sites, this provides the requirement of enabling social influences. Since users can view their friends' activities, as well as learn from the game, better online behaviour will be encouraged. With regards to flow, users are able to choose whether they would like to learn more about the security topics from tutorials or take the quizzes. Users are free to curiously navigate the site. By using the mix of hypertext and multimedia the user's attention is attempted to be sustained and thus interest generated from using the game. The basic intuitive design supports effortless playfulness with the game. As the system will rely on social networks for user control, an intrinsic amount of security has been inherited. In addition, the game is simplistic in nature and thus there are no significant potential security flaws. Overall, the game has been designed taking into consideration the various requirements prescribed by the literature.

## VI. FUTURE WORK

This work involved the development of a conceptual prototype that encapsulated the identified requirements to enhance security awareness. Future work entails the expansion into a functional prototype that can be effectively used as part

of a security awareness programme. In addition, once adequate testing has been completed, the game can be deployed in a social networking site environment.

## VII. CONCLUSION

This paper presents the design of an online game, which utilizes social networking sites, to promote cyber security awareness. Initially, decisions need to be made over hypermedia, multimedia and hypertext to achieve perception, comprehension or projection. The game also incorporates various requirements that promote good game design. These include: comprehensive database of questions, weighted system, use of practical data, automation, dynamics, effort and user acceptance. These principles have been applied in the completion of a prototype. Overall, the designed application aims to create awareness on cyber security topics by using a virtual tool to educate and test users using a social networking environment.

## REFERENCES

- [1] M. Eminagaoglu, E. Uçar and S. Eren, "The positive outcomes of information security awareness training in companies-A case study," *Information Security Technical Report*, vol. 14, pp. 223-229, 2009.
- [2] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computers & Security*, vol. 27, pp. 241-253, 2008.
- [3] E. Kritzing and S.H. von Solms, "Cyber Security for home users: A New Way of Protection through Awareness Enforcement," *Computers & Security*, vol. 29, pp. 840-847, November. 2010.
- [4] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Computers & Security*, vol. 29, pp. 432-445, 6. 2010.
- [5] R.C. Dodge, "Phishing for user security awareness," *Computers & Security*, vol. 26, pp. 73-80, 2007.
- [6] R.S. Shaw, C.C. Chen, A.L. Harris and H. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education*, vol. 52, pp. 92-100, 1. 2009.
- [7] H.A. Kruger and W.D. Kearney, "A prototype for assessing information security awareness," *Computers & Security*, vol. 25, pp. 289-296, 2006.
- [8] C.L. Hsu and H.P. Lu, "Why do people play on-line games? An extended TAM with social influences and flow experience," *Information & Management*, vol. 41, pp. 853-868, 2004.
- [9] D.H. Shin and Y.J. Shin, "Why do people play social network games?" *Computers in Human Behavior*, 2010.
- [10] J. Johnston, J.H.P. Eloff and L. Labuschagne, "Security and human computer interfaces," *Computers & Security*, vol. 22, pp. 675-684, 12. 2003.
- [11] S. Priebatsch, "The game layer on top of the world," vol. Podcast, 2010.
- [12] I. Commtouch, "Internet Threats Trend Report," Commtouch., 2011.
- [13] J. Nielsen, "10 Heuristics for User Interface Design," Available at [http://www.useit.com/papers/heuristic/heuristic\\_list.html](http://www.useit.com/papers/heuristic/heuristic_list.html), Accessed 20110121.
- [14] F.D. Davis, "A technology acceptance model for empirically testing new end-user information systems: theory and results," *Doctoral Dissertation*, Sloan School of Management, Massachusetts Institute of Technology, 1986.
- [15] J.W. Moon and Y.G. Kim, "Extending the TAM for a World-Wide-Web context," *Information & Management*, vol. 38, pp. 217-230, 2001.
- [16] M. Chuttur, "Overview of the technology acceptance model: Origins, developments and future directions," 2009.
- [17] R.B. Cialdini, *Influence: The Psychology of Persuasion*, Collins, 1998, pp. 336.
- [18] M. Csikszentmihalyi, *Flow: The Psychology of Optimal Experience*, Harper Perennial, 1991, pp. 320.
- [19] B.D. Cone, C.E. Irvine, M.F. Thompson and T.D. Nguyen, "A video game for cyber security training and awareness," *Computers & Security*, vol. 26, pp. 63-72, 2. 2007.



[20] The Center for Information Systems Security Studies and Research, INC., "CyberCIEGE Educational Video Game," "CyberCIEGE Educational Video Game," Available at: <http://www.cisr.us/cyberciege/>, Accessed 20110110.

[21] Department of Defence (United States of America), DOD., "CyberProtect," Available at <http://iase.disa.mil/eta/cyber-protect/launchpage.htm>., Accessed 20110110.

[22] S. Khan, "Let's use video to reinvent education," Availabe at [http://www.ted.com/talks/salman\\_khan\\_let\\_s\\_use\\_video\\_to\\_reinvent\\_education.html](http://www.ted.com/talks/salman_khan_let_s_use_video_to_reinvent_education.html), Accessed 20110121.,