Addressing the spectre of phishing: are adequate measures in place to protect victims of phishing?*

Fawzia Cassim[**]

Abstract

The Internet has introduced cheap, interactive and instant global communications. However, it has also resulted in new forms of criminal behaviour. The technique whereby scammers trick bank customers into entering their usernames and passwords is called 'phishing'. Therefore, phishing scams are used to coerce unsuspecting users to disclose personal and banking information about them. Scammers obtain private information about consumers by posing as legitimate businesses and they play on the combination of trust and fear of fraud. Phishing attacks exploit vulnerabilities in computer networks, cause financial loss to victims and banking institutions and undermine consumer confidence in e-commercial transactions.

However, attempts are being made by some countries and organisations to tackle phishing on a global scale. In this article, I shall examine the increase in phishing attacks in South Africa and the United States of America and measures taken to address phishing in these countries. The United States has invaluable experience in combating phishing; hence it was chosen for the comparative study. The role of international bodies in addressing phishing and the effectiveness of new developments on phishing attacks will also be discussed. The study reveals that both the United States of America and South Africa have introduced legislation that can be used to address phishing. However, it is submitted that such legislation can be improved upon. It is recommended that more comprehensive legislation to address phishing should be introduced in South Africa. At the end of the day, the

---

* This article is based on research undertaken at the University of Berkeley, California during May 2014 in terms of a Foreign General Research Grant awarded by the Research and Innovation Committee, College of Law, Unisa.

** BA (Law) (UDW) LLB (UN); LLM (Unisa) LLD (Unisa). Admitted attorney and conveyancer. Associate Professor: School of Law, University of South Africa.

need for a multi-faceted approach involving law enforcement agencies, legislators and the private sector is advocated, as phishing scams impact on governments, companies and individuals worldwide.

INTRODUCTION

The Internet has created a vibrant marketplace for businesses and consumers to interact but it has also provided criminals with new avenues to commit crimes.[1] Although the Internet allows inexpensive, interactive and instant global communications, it does not exist in a legal vacuum. The Internet poses a number of problems in a broad spectrum of legal areas such as freedom of expression, intellectual property, criminal law, contracts and jurisdiction.[2] Moreover, the vulnerability of computer systems and networks to unauthorised users facilitates criminal activity on the Internet.[3] The theft of information is becoming easier for cyber criminals who now have greater access to consumer information stored on databases. Cyber attacks have also increased in regularity and severity as cyber criminals have become more sophisticated and brazen.[4] Thus cyber crime has become the fastest growing crime in the world with resourceful crime syndicates preying on millions of unsuspecting and gullible victims. Nowadays, perpetrators can use fraudulent e-mails and fake websites to scam unsuspecting victims around the globe. This form of online fraud can be distinguished from physical fraud because of the difficulty to identify and apprehend online fraudsters and the ease with which such crimes can be committed.[5] Thus, the anonymity of cyberspace has facilitated phishing scams.

---

1 Stevenson 'Plugging the 'phishing' hole: legislation versus technology' (2005) 5 *Duke Law and Technology Review* 1–14 at 1. This article analyses the Anti-Phishing Act of 2005 which was aimed at curbing phishing. The writer concludes that technological solutions are the most effective means of reducing or eliminating phishing attacks. Also see Nuth 'Taking advantage of new technologies: for and against crime'(2008) 24 *Computer Law and Security Report* 437–446 at 437–438.

2 Rubin *et al* 'US and international law aspects of the Internet: fitting square pegs into round holes' (1995) 3/2 *International Journal of Law and Information Technology* 117–143 at 118.

3 *Id* at 125.

4 Nuth n 1 above at 437–438.

5 Fraud was said historically to involve face-to-face communication because physical contact was necessary. Chawki 'Phishing in cyberspace: issues and solutions' 2006 *Computer Crime Research Center* 2. The Internet is said to be responsible for 'borderless fraud' and fraudsters are using the Internet to trick and deceive unsuspecting victims for the purpose of financial gain. See Goodman & Brenner 'The emerging consensus on criminal conduct in cyberspace' 2002 *International Journal of law and Information Technology* 139–223 at 147.

Phishing is regarded as the most common type of online fraud.[6] According to the Anti-Phishing Working Group, phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal the personal identity data of customers and their financial account information.[7] Phishing refers to criminal acts that are carried out online to coerce victims to disclose personal or secretive information about themselves.[8] A phishing attack thus involves two victims: the business sector and the consumer. The term 'phishing' originated around 1996, and it was initially used to describe the use of e-mails as bait to 'phish' for passwords and financial data from 'a sea of Internet users'.[9] The first well-known

---

6 Ravin 'Avoiding online identity theft and representing its victims' December 2008 *New Jersey Lawyer* 60–65 at 60.

7 See Anonymous 'APWG' at: http://www.antiphishing.org/ (last accessed on 17 June 2014). Also see Vittal 'Phishing: the scourge of the internet' 2006 8(3) *Tort Source* 2; Nykodym *et al* 'Cybercrime and business: how to not get caught by the online phisherman' (2010) 5(4) *Journal of International Commercial Law and Technology* 252–259 at 252–253 and Sullins ' "Phishing" for a solution: domestic and international approaches to decreasing online identity theft' 2006 *Emory International Law Review* 397– 433 at 397–398.

8 Phishing involves two separate acts of fraud namely, the phisher first steals the identity of the business it is impersonating and then acquires the personal information of the unsuspecting customer who falls for the impersonation; hence the reference to phishing as 'two-fold scam' and a 'cyber crime double play' by certain commentators. See Stevenson n 1 above at 3. For further definitions of phishing, see *inter alia*, Anonymous 'Phishing' at: http://www.F:/phishingActionFraud.5/5/2014.html (last accessed on 5 May 2014); Davis 'How to prevent and, if necessary, respond to a phishing attack' (2005) 23(4) *IPL Newsletter* 44–45 at 44; Nykodym *et al* n 7 above at 252; Chawki n 5 above at 1; Lynch 'Identity theft in cyber space: crime control methods and their effectiveness in combating phishing attacks' (2005) 20 *Berkeley Technology Law Journal* 259–300 at 259; Sullins n 7 above at 400–401; Savirimuthu 'Identity theft and the gullible computer user: what Sun Tzu and the *Art of War* might teach' (2008) 3(2) *Journal of International Commercial Law and Technology* 120–128 at 121. Also see Hughes 'A report on the safe use of the internet: some of the most common risks' (2008) 91(2) *Hispania* 408–411 at 409; Black 'Phish to fry: responding to the phishing problem' (2005) 16 *Journal of Law, Information and Science* 73–91 at 74; Almahroos 'Phishing for the answer: recent developments in combating phishing' 2007–2008 *Journal of Law and Policy* 595–621 at 596; Cherry 'The effect of spyware and phishing on the privacy rights of Internet users' 2005–2006 *Journal of Law and Policy* 573–598 at 593. For more information, see the section on 'Defining phishing' below.

9 The 'ph' is linked to popular hacker naming conventions. It is believed to arise from the word 'phreaking' which is a form of hacking telephone lines. See Gercke *Understanding cybercrime: a guide for developing countries* (ITU Publication 2011) 119. Also see Lynch n 8 above at 259. Also see Feigelson & Calman 'Liability for the costs of phishing and information theft' (April 2010) 13(10) *Journal of Internet Law* 15–25 at 15; Nykodym *et al* n 7 above at 253; Sullins n 7 above at 401–402; Black n 8 above at 75; Calman 'Bigger phish to fry: California's anti-phishing statute and its potential imposition of secondary liability on internet service providers' (2006–2007) 13(1) *Richmond Journal of Law and Technology* 1–24 at 5–6; Ravin n 6 above at 60–61.

instance of phishing took place in 1996 when criminals compromised American Online (AOL) accounts by falsely obtaining passwords from AOL users.[10]

The popularity of online commerce sites is said to be responsible for the rise in phishing.[11] Scammers obtain private information about consumers by posing as legitimate businesses and consumers are tricked in this manner.[12] E-mail phishing attacks are the most common attacks. They occur when offenders identify legitimate companies, such as financial institutions which offer online services and communicate electronically or directly with their customers whom phishers can target. Websites are designed to look like legitimate websites (called 'spoofing sites') requiring victims to perform normal 'log in' procedures. This enables offenders to obtain personal information such as account numbers and online banking passwords.[13] Offenders use the personal information to log in to victims' accounts and commit offences such as the transfer of money, applications for passwords or new accounts. Phishers can reap significant rewards from their victims and the ability to launch simultaneous attacks makes this criminal activity attractive. The increase in phishing attacks demonstrates its success. However, phishing attacks are not limited to accessing passwords for online banking only. Offenders may also seek access codes to computers, auction platforms and personal identity numbers (social security numbers in the United States) which may facilitate identity theft offences.[14] Phishing not only causes financial loss to its victims but it undermines consumer confidence in e-commerce transactions.[15] Although banks have introduced information technology to provide services to their customers, cyber criminals are undermining this technology by committing theft.[16] Thus, these phishing attacks exploit vulnerabilities in computer networks, impact on consumers, corporations and Internet commerce worldwide and make monitoring, detection and capture of offenders more difficult.

---

10 Nykodym *et al* n 7 above at 253. Also see Feigelson and Calman n 9 above at 16.

11 Ziring 'Revoking the license to phish: providing civil remedies for victims of online fraud' (2006) 37 *McGeorge Law Review* 174–178 at 174.

12 *Ibid*. Also see Calman n 9 above at 1.

13 *Ibid*. Also see Ravin n 6 above at 61.

14 Rubin *et al* n 2 above at 120.

15 See Davis n 8 above at 44; Lynch n 8 above at 260, 266 and Sullins n 7 above at 398.

16 Mason 'Electronic banking and how courts approach the evidence' 2013 *Computer Law and Security Review* 144–151 at 144. The article examines the burden of proof in banking cases.

South African banks have also become vulnerable to cyber crime or computer crime. Concern has been expressed by South African banks and software security companies about the increase in phishing schemes.[17] Millions of adults are reported to have fallen victim to identity theft with phishing being increasingly used to obtain personal information.[18] Many of the phishing operations are said to be part of the Nigerian '419' scam.[19] Russia and Estonia are also regarded as common locations where most phishing schemes originate.[20] However, organisations such as the South African Banking Risk Information Centre (SABRIC) are combatting cyber crime in the South African banking industry.[21]

The article will examine the increase in phishing attacks in South Africa and the United States of America, and measures taken to address phishing in these countries. The United States of America was chosen for the comparative study because it has more experience in dealing with phishing cases and legislation has been introduced at both federal and state levels to address phishing scams.[22] The aim of this comparative study is to ascertain whether there are legal principles which can be used as guidelines in order to find possible solutions for the position in South Africa. The effectiveness of new developments in addressing phishing attacks will also be discussed. Strong laws addressing phishing scams are necessary to restore consumer

---

17 Moodley-Isaacs 'Crafty cyber-crooks going all out to rob you' *The Saturday Star* 1 May 2010 at 1.

18 Bielski 'Phishing phace-off' Sept 2004 *ABA Banking Journal* 46–54 at 48.

19 Cassim 'Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players' 2011 *CILSA* 123–138 at 136.

20 Anonymous 'Bank liable for losses in phishing scheme' (Aug 2011) 45(8)*The Bankers Letter of the Law* 1–6 at 1. It is noteworthy that law enforcement agencies have also traced sources of attacks to Europe, Eastern Europe, Asia and the US. See Bielski n 18 above at 48; Sullins n 7 above at 418 and Lynch n 8 above at 268–269. Also see Cajani 'International phishing gangs and operation phish & chip' (2009) 6 *Digital Evidence and Electronic Signature Law Review* 153–157, regarding the successful cooperation between prosecution authorities in Italy and Romania, to investigate phishing operations originating in Romania and Russia targeting Italian banks. This cooperation resulted in successful arrests and convictions.

21 SABRIC is a wholly owned subsidiary of the Banking Association of South Africa funded by the major banks in South Africa. It was established in 2002 to address bank-related crime through effective public private partnerships. For further information, see https://www.sabric.co.za (last accessed on 8 July 2014).

22 As stated earlier, the first well-known instance of phishing involving AOL users took place in the United States of America (USA) in 1996. This demonstrates that the USA has invaluable experience in dealing with phishing attacks. The discussion on 'United States of America' below will elaborate further on legislative measures introduced at federal and state levels to combat phishing.

confidence in the Internet. The computer industry and the banking industry also need to stay abreast of the crafty cyber criminal and develop technical solutions to address the problem. Internet users should also be educated about the risks of transacting online, and they need to practice caution and vigilance when transacting online. The study reveals that both the United States of America and South Africa have introduced legislation that can be used to address phishing. However, the need for a more comprehensive legislative framework encompassing legal, regulatory and technical approaches is advocated as phishing scams impact on governments, companies and individuals worldwide. At the end of the day, a comprehensive, combined and co-operative effort from all role players (law enforcement agencies, legislators and the private sector) is needed to address the phishing problem.

DEFINING PHISHING

The United States Department of Justice defines phishing as the use of e-mails and websites by criminals to trick Internet users into disclosing their financial or personal information.[23] Phishing refers to the act of sending an e-mail to a user falsely claiming to be a bank or a legitimate organisation or company with the intention to coax the user into surrendering private information about him or her or his or her company.[24] Thus, phishing schemes utilise pretext e-mails sent to unsuspecting consumers, and phishers pose as a trusted entity such as a financial institution, an Internet service provider (ISP) or a government agency.[25] Such phish mails usually contain links to unauthorised web pages created by crafty criminals requesting personal information such as identity numbers or social security numbers or passwords.[26] Phishing works if the recipient of the bogus e-mail acts on the

---

23 Stevenson n 1 above at 1.

24 Anonymous n 20 above at 1. Also see Feigelson & Calman n 9 above at 16. For additional definitions of 'phishing', see Nuth n 1 above at 439; Reach 'Do you know if your computer is safe?' October 2009 *Bar Leader* 12–13 at 12; Hamman 'Phishing in the world wide web ocean: *Roestoff v Cliffe Dekker Hofmeyr Inc* – a case of cyber laundering through an attorney's trust account' (2013) 17 *Law, Democracy and Development* 49–63 at 51; The Anti-Phishing Working Group, 'Proposed solutions to address the threat of e-mail spoofing scams' at: http://www.antiphishing.org/ (last accessed on 17 June 2014). The Anti-Phishing Working Group (APWG) is an industry association which focusses on eliminating identity theft and fraud that result from the growing problem of phishing and e-mail spoofing. Regarding features of phishing attacks see Black n 8 above at 76–77.

25 Feigelson & Calman n 9 above at 16.

26 Bielski n 18 above at 46.

message it transmits.[27] The cyber criminal will then use the fraudulently obtained information to commit fraud[28] or identity theft. E-mails from phishers usually play on the user's fear of fraud and fear of one's account been compromised or terminated.[29] Thus phishing occurs when criminals exploit a weak link in the online security chain, namely, the individual users.

EXAMPLES OF PHISHING

Phishing scams tend to focus mostly on banks and online shopping sites. It has also emerged that most phishing attacks are launched by organised criminal gangs and sophisticated computer users.[30] The following are common examples or methods of phishing: the Nigerian scam ('419' scam) which involves the use of e-mails to dupe gullible Internet users to part with their money; the dragnet method which involves the use of spammed e-mails which contains false corporate identification to scam customers or consumers; the rod and reel method whereby phishers identify specific victims in advance and convey false information to lure them to disclose personal and financial information; the lobsterpot method which relies on the use of spoofed websites to hijack unsuspecting victims; and the gillnet phishing technique whereby phishers introduce malicious codes into e-mails and websites to change settings in user systems and or transmit data fraudulently obtained to other phishers for later illegal access to user financial accounts.[31] Spear phishing occurs when phishers target users who have actually done business with the specific institutions.[32] Criminals have thus created innovative ways to scam innocent users. Fraudsters also place spyware in the phishing e-mail which scans the user's desktop.[33] This enables the criminals to obtain access to the user's computer. Phishers also use 'pop ups' and 'pop under' pages by manipulating the HTML code to appear authentic and this deludes the user.[34] Pharming or domain spoofing involves the use of Trojan horse programmes that compromise the user's computer or domain name system (DNS) server to reroute Internet users

---

27 Reach n 24 above at 12.

28 According to Snyman, fraud refers to the 'unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another'. See Snyman *Criminal law* (5ed 2008) 531.

29 Feigelson & Calman n 9 above at 16.

30 Savirimuthu n 8 above at 125.

31 For more information on the different phishing techniques and methods, see Chawki n 5 above at 2–3; Lynch n 8 above at 267–270. Also see Nuth n 1 above at 439.

32 Spear phishing entails an apparent request from a department in your organisation. *Ibid*.

33 Bielski n 18 above at 46.

34 *Ibid*.

from the desired Internet site to an illegitimate site, whilst vishing involves criminals sending spoof e-mails to unsuspecting businesses and individuals.[35] A phishing and hacker subculture has also now arisen with phishing kits now available online. These phishing toolkits are being used to professionalise fraud attacks.[36] Available phishing tools include malicious software, web hosting for phishing web sites, botnets rentals and phishing kits that facilitate phishing.[37]

Identity theft is also a form of phishing.[38] The Identity Theft and Assumption Deterrence Act of 1998 in the United States, describes identity theft as the process when a person knowingly transfers or uses without lawful authority, a means of identification of another person with the intent to commit or to avoid or abet any unlawful activity that constitutes a violation of federal law or a felony in terms of any state or local law.[39] Phishers use information obtained via their scams to commit identity theft and fraud.[40] The fraudster obtains vital information such as the identity number, credit card number and social security number, and this information is used to obtain credit and purchase merchandise and services in the victim's name.[41] Identity theft causes financial loss to consumers, creditors and financial institutions.

Thus, banks and Internet users can become victims to phishing schemes. This requires urgent responses by *inter alia*, the banking industry and the computer industry.

---

35 It is noteworthy that the phrase 'vishing' emerged as a 'twist' on traditional phishing. A fake subpoena or invoice directed at the head of a company is called whaling. These attacks are called 'social engineering' because they rely on someone who unknowingly discloses private information. See Savirimuthu n 8 at 121; Reach n 24 above at 13 and Almahroos n 8 above at 598–599.

36 Nykodym *et al* n 7 above at 253.

37 Fiegelson and Calman n 9 above at 18.

38 The Anti-Phishing Working Group (APWG) also regards phishing as a form of online identity theft. Lynch n 8 above at 265; 278–284; Nuth n 1 above at 439.

39 See 18 USC section 1028 (a) (7). Also see Pierson 'Understanding identity theft and stopping the crime' March 2007 *The Computer and Internet Lawyer* 22–26 at 22. For more information on identity theft, see *inter alia,* Anonymous 'FBI-Identity theft' at: http://www.fbi.gov/about/investigater/cyber_theft/identity-theft-overview (last accessed on 6 May 2014); Hoofnagle 'Identity Theft: making the known unknowns known' (2007) 21(1) *Harvard Journal of Law and Technology* 98–122; Lynch n 8 above at 260; Newman *Identity Theft* US Department of Justice Problem-Oriented Guides for Police Problem-Specific Guides Series (No 25 June 2004).

40 Sullins n 7 above at 401.

41 Sullins n 7 above at 402 and Feigelson & Calman n 9 above at 16.

THE HARMFUL EFFECTS OF PHISHING

The success of phishing scams can be attributed to a combination of trust and fear.[42] Phishing scams impact on the security of individuals, companies and the Internet. It is difficult to deter because normal barriers to offline crime do not apply and the anonymity of computer crime facilitates the success of phishers.[43] Damages occur when the criminals use the stolen data to purchase items or withdraw money from the victims' existing accounts, to open bank or credit card accounts in the victims' names and they use the fraudulent e-mails to spread computer viruses that send out phishing e-mails to more people.[44]

Phishing has created havoc in cyber space impacting on online commercial transactions. In the case of *Experi-Metal v Comerica*,[45] the Michigan federal court held that the bank was liable to one of its customers for losses suffered when it became a victim of a phishing scheme. The court found in favour of the plaintiff firm as the bank Comerica had failed to discharge the burden of good faith. Moreover, the court found that the bank should have detected or stopped the fraudulent wire activity earlier.[46] European businesses were also recently targeted by phishers in an instance involving gas emission allowances.[47] Governments such as Belgium and Britain had fallen victim

---

42 The phisher creates the appearance of being a trusted source, and thus attempts to frighten the recipient into providing the confidential information to the so-called trusted source. Black n 8 above at 77.

43 Lynch n 8 above at 271. Also see Almahroos n 8 above at 601.

44 Sullins n 7 above at 402.

45 US DC (for the Eastern district of Michigan) Case 09–14890 June 13 2011. The comptroller at a Michigan firm inadvertently provided a third-party with immediate online access to the company's bank accounts during January 2009. This resulted in the fraudster initiating wire transfer payment orders totalling $1,901,269 using the comptroller's user information in a matter of few hours. The payment orders were directed mostly to accounts held at banks in Russia and Estonia. The American bank Comerica halted the bogus wire transfers and tried to reverse them when the fraud was detected.

46 Anonymous n 20 above at 1. *Ibid.*

47 According to the European Union's Emission Trading System, companies that are large emitters of greenhouse gases must have sufficient allowance or credit to cover the CO2 they release annually. National authorities issue the credits and businesses can trade their credits to other businesses that require them. Crafty cyber criminals sent e-mails to firms in Europe that appeared to emanate from the German Emissions Trading Authority. Such firms were requested to re-register on the agency's Web site to avoid the threat of a hacker attack. Nykodym *et al* n 7 above at 255. Also see Markus *et al* 'Phishing of European emission allowances and resulting legal implications' (2012) 3 *Carbon and Climate Law Review* 228–245.

to the above scam when they purchased emissions allowances from the cyber criminals.[48] However, there have been some successful prosecutions: A Florida man was indicted in Pennsylvania for a phishing scam that mimicked a Hurricane Katrina relief website; in 2004, Zachary Keith pleaded guilty in a Texan federal court to crimes relating to phishing activity and received 46 months' imprisonment; the United States (US) Department of Justice has also successfully prosecuted other defendants in US courts.[49]

However, banks can become more pro-active by addressing the problems, by investigating solutions and investigating filter controls and introducing best practices for online marketing and e-mail alerts.[50] Banks should invest in anti-phishing technology to address phishing attacks. There should also be cross-industry collaborative initiatives to combat e-mail phishing schemes such as those initiated in the United States.[51] Cyber forensics can also be used to detect and avert phishing schemes. However, the ability of the cyber criminal to 'up the ante' all the time means that law enforcement has to play catch up all the time. The hacking of many servers who are victims of phishing schemes also exacerbates the detection of the phishing schemes.

LIABILITY FOR COSTS OF PHISHING

The results of phishing attacks can be quite lucrative for phishers.[52] The phishers gain access to banks and social networks using the customers' accounts. The information is also sold to the cyber underground network leading to more attacks. The costs of phishing arise not only from the monetary loss to consumers and businesses, but also include monies spent on devising technical solutions to counteract phishing.[53] This cost is then passed onto the consumers who purchase the products and services to protect themselves. This results in an escalation of costs on consumers.[54]

Some companies do not report losses to cyber crime because they fear loss of consumer confidence and stock price reductions.[55] In other instances, companies only learn about the security breaches after the cyber crime has

---

48 Nykodym *et al* n 7 above at 255.
49 Calman n 9 above at 9–10.
50 Bielski n 18 above at 50, 54.
51 For example, see the Anti-Spam Technical Alliance. See Bielski n 18 above at 48.
52 See Lynch n 8 above at 270 and Black n 8 above at 78.
53 Nykodym *et al* n 7 above at 255.
54 Stevenson n 1 above at 2.
55 Sullins n 7 above at 476.

been reported.[56] Some laws may prohibit fraud and unlawful business practices but they do not directly address phishing.[57] Therefore, it is important to provide civil remedies to consumers and Internet Service Providers (ISPs) who are adversely affected by phishing schemes. Phishing tends to undermine consumer confidence in the integrity of personal information transmitted via the Internet; therefore any action taken against fraudulent activities will rebuild confidence in the security of Internet commerce.[58]

Some banks compensate their clients for losses incurred as a result of the phishing scheme through no negligence of the client.[59] However, the question arises whether the victim's time and effort in dealing with the theft should be compensated. United States federal law calls for restitution by convicted phishers including reasonable remediation costs incurred by customers.[60] However, there is no guarantee that convicted criminals will have the means to compensate the banks and victims fully.

REGULATING PHISHING: A REVIEW OF MEASURES OR STRATEGIES TO CURB PHISHING IN SELECTED JURISDICTIONS

Many countries have tried to update their laws as phishers have become more sophisticated. The speed and anonymity of the Internet compounds the problem of detection. It has been mooted that any legislation which seeks to punish Internet-related offences or crimes needs to overcome three hurdles, namely, the difficulty inherent in finding the perpetrator of an online crime, obtaining personal jurisdiction and enforcing the judgment.[61] Therefore, it is important to find the perpetrator, obtain jurisdiction and enforce the judgment to combat the phishing problem. Collaboration between government, private business entities, international organisations and potential victims is also needed.

---

56 See Black n 8 above at 78 and Lynch n 8 above at 266.
57 Sullins n 7 above at 413.
58 Ziring n 11 above at 175.
59 Feigelson & Calman n 9 above at 19.
60 Feigelson & Calman n 9 above at 15.
61 For a detailed discussion about these hurdles, see Stevenson n 1 above at 6–9.

South Africa

Recent concerns have been raised about online banking in South Africa.[62] It has been reported that South Africa has become a top target for phishing attacks in Africa.[63] South Africa is said to be witnessing more attacks than previous years because of the increase in Internet penetration and broadband accessibility in the country. The lack of a clear cyber security strategy has also exacerbated the situation.[64] Cyber criminals use fraudulent swapping of cell phone SIM cards to clear out their victims' bank accounts, including home loan accounts.[65] After receiving the victim's details in a phishing attack, fraudsters illegally swap the SIM card to prevent the victim from receiving notification from his or her bank that beneficiaries have been added to his or her Internet banking profile and that a transaction has been made on his or her account.[66] However, mobile operators maintain that they are not liable for fraud committed on customers' bank accounts.[67] In the case of *Nashua Mobile (Pty) Ltd v GC Pale CC t/a Invasive Plants Solution*,[68] it was held that a SIM swap does not in itself enable a fraudster to commit fraud on a customer's bank account. The Independent Communications Authority of South Africa (ICASA) which regulates cell phone providers, has stated that it has no jurisdiction over cell phone providers who fail to comply with the Regulation of Interception of Communications and

---

62 Anonymous 'Fresh concerns over online banking' at: http://www.elaw@legalbrief.co.za (last accessed on 10 April 2013).

63 Anonymous 'SA top target for phishing attacks' at: http://www.elaw@legalbrief.co.za (last accessed on 8 May 2013); Anonymous 'SA is the second most targeted for phishing attacks' at: http://www.itnewsafrica.com/2014/04 (last accessed on 8 July 2014).

64 *Ibid*.

65 Anonymous 'How crooks use SIM swaps to rob you' at: http://www.forensic@legalbrief.co.za (last accessed on 2 May 2013). There have also been arrests in the Vodacom banking fraud case, where a syndicate targeted the four major banks, Standard Bank, Nedbank, Absa, FNB and Capitec. Clients were defrauded when their banking details were stolen through phishing. See Anonymous '3RD arrest in phishing case' at: http://www.news24.com (last accessed on 8 July 2014).

66 Ardé 'Cyber crooks use illegal SIM swaps to rob you' *Saturday Star* 27 April 2013 at 1.

67 Ardé 'Online bank fraud: the case for 'partial' liability of mobile operators' *Saturday Star* 11 May 2013 at 3.

68 (A3044/2010) [2010] ZAGP JHC 112; 2012 (1) SA 615 (GSJ) (18 November 2010). In this case, GC Pale CC had more than R160 000 stolen from its account via Internet banking fraud following a phishing attack and a fraudulent SIM swop, and it sued Nashua Mobile for damages in terms of the law of delict. The court dismissed the case and found *inter alia*, that the loss experienced by GC Pale CC was too remote to impute liability to Nashua Mobile.

Provision of Communication Related Information Act 70 of 2002 (RICA).[69] However, both the Ombudsman for Banking Services and attorney firms have criticised this stance.[70]

The South African Banking Risk Information Centre (SABRIC) has also warned consumers to be aware of a new software identity scam whereby consumers are tricked into disclosing their personal information.[71] The scam targets home computer users and masquerades as legitimate telephonic calls from reputable computer software stores. The scammers advise victims that their computer systems are faulty or compromised and that their computers require urgent action. During these telephonic calls, the victims are tricked into divulging their personal information and to unwittingly install or accept malware on their computers.[72]

Recently South African municipalities were duped by a scam by an international grant facilitator.[73] The municipality entered into agreements with a company, Metro Grant Holding Corporation to receive 'free' development funding between $2billion and $5billion (about R22 billion to R53billion).[74] In another phishing scam, Standard Bank customers were targeted when claims were placed on new debit orders on their accounts to Liberty Life Insurance. The e-mail was confirmed to be part of a phishing scam and the website was shut down.[75] The South African Revenue Service (SARS) has also posted alerts about scams and phishing attacks on its website in the light of a spate of recent fraudulent e-mails purporting to come from SARS, aimed at enticing unsuspecting taxpayers to part with personal information and their bank account details.[76]

---

69 See Ardé n 66 above at 1. It should be noted that RICA regulates cell phone-related fraud.

70 *Ibid*. Also see Ardé n 67 above at 3.

71 See Anonymous 'Warning over new software identity theft scam' at: http://www.elaw@legalbrief (last accessed on 10 April 2013).

72 *Ibid*.

73 Anonymous 'Top municipal officials fall for 419 scam offering 'free' millions' at: http://www.forensic@legalbrief.co.za (last accessed on 24 April 2014).

74 The municipalities failed to realise that the funding was greater than the South African national budget. *Ibid*.

75 Anonymous 'Cybercrime' at: http://www.elaw@legalbrief.co.za (last accessed on 26 March 2014).

76 Anonymous 'SARS' at: http://www.sars.govt.za (last accessed on 8 July 2014).

In *Roestoff v Cliff Dekker Hofmeyr Inc,*[77] an amount of R350 000 was fraudulently transferred out of the plaintiff's personal account, and R200 000 was 'stolen' from the trust account of the defendant firm. One of the directors of the firm believed that the firm was receiving payment of a debt due to one of its clients. However, the client used the attorney firm's trust account as a conduit to decontaminate the criminal proceeds of the phishing scam. This case illustrates how attorneys can unknowingly become victims of money launderers as a result of phishing scams.

Unlawful electronic fund transfers are a common occurrence in South Africa. This makes cyber security an important priority as it has a detrimental effect on the economy and the most vulnerable people of the country. The advent of cyber security policy is urgently required to address *inter alia,* national security threats in cyber space, cyber crime and develop, review and amend existing substantive and procedural laws to ensure alignment and build confidence and trust in the secure use of information communication technologies (ICTs).[78]

The establishment of organisations such as SABRIC and the role of the South African Ombudsman for Banking Services to combat cyber crime in the banking industry are positive steps in combating phishing. The following legislation can be used to address phishing scams.

The Electronic Communications and Transactions Act 25 of 2002 (ECT)

The main aim of the ECT is to 'provide for the facilitation and regulation of electronic communications and transactions in the public interest'. Cyber crime is addressed in Chapter 13 of the ECT. The ECT has introduced new crimes such as anti-cracking (anti-thwarting) and hacking law which prohibit the selling, designing or the production of anti-security circumventing technology.[79] E-mail bombing and spamming is regulated in sections 86(5) and 45 of the ECT and extortion, fraud and forgery is addressed in section 87.[80] The criminal provisions in section 89 have been criticised as they are

---

77 (34306/2010)[2011] ZAGPPHC 219 (2012); 2013(1) SA 12 (GNP). For a detailed discussion about the case, see Hamman n 24 above at 49–63.

78 Anonymous 'Cybercrime: SA conviction rate at 89%' at: http://www.elaw@legalbrief.co.za (last accessed on 11 July 2012).

79 See ss 86(4) and 86(3) of the ECT.

80 Also see Snail 'Cybercrime in South Africa – hacking, cracking and other unlawful online activities' 2009 *Journal of Information Law and Technology Law* at: http://go.warwick.ac.uk/jilt/2009-1/snail (last accessed on 8 May 2014).

not stringent enough.[81] To illustrate this, section 87 prescribes a fine or imprisonment not exceeding five years. More stringent penalties are required to deter cyber criminals.

The question arises whether perpetrators responsible for phishing schemes can be prosecuted in terms of the ECT. It is noteworthy that the ECT does not address the crime of phishing *per se.* However, as phishing involves Internet fraud, it can fall within the ambit of sections 86 and 87. In instances where the offender uses a skimming device to breach certain security measures, and he or she uses the data enclosed within the magnetic strip of a debit or credit card illegally or unlawfully, then the offender has contravened sections 86 or 87 of the ECT. Similarly, offenders may infringe the common law offence of fraud because they are guilty of committing fraudulent transactions by using the cloned debit or credit card.

The Protection of Personal Information Act 4 of 2013 (POPI)

This legislation was signed into law during November 2013. It promotes *inter alia*, the protection of personal information processed by private and public bodies and provides for the protection of the rights of persons regarding unsolicited electronic communications. The Act regulates identity theft: the perpetration of Internet banking fraud whereby the criminal uses personal information of the customer or user to open new accounts.[82] The new legislation places a responsibility on companies to respect the personal information of clients and to handle such information with utmost care and responsibility.[83] POPI provides for penalties by companies in the event of non-compliance: fines of up to R10 million or imprisonment of up to 10 years.[84] Companies are also held liable if the data of clients is obtained to

---

81 The Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 (RICA) is said to prescribe much harsher measures. See Van der Merwe *et al Information and communications technology law* (2008) 75–78.

82 It should be noted that one of the purposes of POPI is to 'regulate the manner in which personal information may be processed by establishing conditions prescribing minimum standards for the lawful processing of personal information'. Chapter 3 of POPI addresses the conditions for lawful processing of personal information. Also see Thakali 'New legislation comes too late for identity theft victims' *Saturday Star* 30 November 2013 at 7.

83 See s 19 of POPI.

84 Section 107 of POPI addresses penalties whilst s 109 of POPI addresses fines. Also see Thakali n 82 above at 7. For further discussion about POPI, see Luck 'POPI – Is South Africa keeping up with international trends?' May 2014 *De Rebus* 44–46.

clone one's identity.[85] Thus, all public and private organisations will have to put systems in place to protect their client's personal information.[86] Similarly, companies that you do business with, cannot now divulge personal information to other companies for marketing purposes.[87]

POPI thus will compel organisations such as PASA (the Payment Association of South Africa which regulates online transactions) to secure the integrity of personal information in their possession or under their control, by taking appropriate and reasonable technical and organisational measures to prevent the loss of personal information and unlawful access to personal information. These companies will thus be forced to implement generally accepted information security practices and procedures to protect personal information in terms of section 19 of the Act. Non-compliance with the provisions of the Act will expose companies to complaints being lodged with the Information Protection Regulator,[88] and possible criminal fines and civil damages claims from individuals.[89] It will be interesting to see how the courts will rule on future POPI transgressions.

INTERNATIONAL LAW

United States of America

Many phishers operate outside the United States but they can be prosecuted in the United States. Such prosecutions depend on increased cooperation between the United States and other countries.[90] Internet crimes are regarded as federal offences because of their national and international nature.[91] Internet crime is seen as the responsibility of the federal government and as such, should be undertaken in cooperation with the law enforcement agencies of other countries.[92] The Federal Bureau of Investigation (FBI) is using their investigation skills, knowledge of forensics and international relations to fight cyber crime. The FBI has been successful in indicting people on charges of conducting financial fraud based on phishing.[93] The

---

85 See s 19 of POPI.
86 See ss 21 and 69 of POPI.
87 See ss 19 and 69 of POPI.
88 See ss 40 and 74 of POPI, which address the powers and duties of the Information Protection Regulator and the procedure to lodge complaints respectively.
89 See ss 107 and 99 of POPI.
90 Such as Romania, Poland and the United Kingdom. Feigelson & Calman n 9 above at 17.
91 Rubin *et al* n 2 above at 127.
92 *Ibid*.
93 Operation Phish Fry was used to arrest a number of defendants. About $2 million was stolen from victims with accounts at the Bank of America and Wells Fargo. Bank

FBI and the Department of Justice (DOJ) are also involved in the investigation and prosecution of computer crime through its Cyber Division, Internet Crime Complaint Centre (FBI) and Computer Crime and Intellectual Property Section (DOJ).[94] American authorities have also experienced some success with the apprehension of phishers such as Jeffrey Goodin during 2007 and Michael Dolan and Daniel Maschia during 2008.[95] Whilst federal agencies such as the Justice Department and FBI are involved in efforts to address phishing attacks and protect consumers, there is a need for these government agencies to work with other organisations, private business entities, potential victims, law enforcement agencies, state and federal legislatures and software manufacturers to ensure that crime control is effective.[96]

Some victims and companies do not report the crime of phishing to avoid reduction in public trust and this may be detrimental to law enforcement. The anonymity of international transactions further exacerbates the apprehension of phishers.[97] Increasing consumer awareness and anti-phishing technology may reduce the effectiveness of phishing. Whilst financial institutions usually cover the loss for liability to their customers, the question also arises whether Internet Service Providers (ISPS) should be held liable for phishing as they provide phishers with e-mail access and web space. Whilst some states such as California have debated whether ISP-providers can face secondary liability, other states specifically prohibit liability for phishing on ISP providers.[98] It has also been mooted that settlements may assist individual victims who have suffered major harm.[99]

---

customers clicked on e-mail messages that sent them to fake Web sites made to look like the actual banking site. Cyber criminals used sensitive data typed by customers (such as usernames and passwords) to transfer funds into their own accounts. Nykodym n 7 *et al* above at 256. The FBI is also collaborating with other agencies to arrest and prosecute identity thieves. See Lynch n 8 above at 265; 272–273.

94 For more on the roles of the FBI and DOJ, see Kim *et al* 'Computer crimes' (2012) 49 *American Criminal Law Review* 444–486 at 479–481.

95 Feigelson & Calman n 9 above at 17.

96 For a discussion about the roles of different agencies and or role players, see Lynch n 8 above at 273–274.

97 See Calmon n 9 above at 10, Almahroos n 8 above at 601 and Lynch n 8 above at 271.

98 Feigelson & Calman n 9 above at 20.

99 *Id* at 21.

Large tech companies such as Google, Facebook and Microsoft have united to combat e-mail scams and phishing.[100] To combat phishing scams, major technology and financial companies in the US have formed an organisation to design a system for authenticating e-mails from legitimate senders and removing fake e-mails.[101] The new system is called DMARC (Domain-based Message Authentication, Reporting and Conformance), which is designed to verify that an e-mail actually came from the sender in question.[102] According to Rubin *et al*, cyber crime legislation can only hope to achieve its purpose if it confronts Internet anonymity.[103] This requires an active role in eliminating opportunities for crime by both individual users and computer system operators. To this end, unauthorised network access can be prevented by a combination of electronic defences such as encryption, firewalls and one-time passwords with contractual safeguards and the enforcement of clear corporate policy.[104] However, the current security measures have been criticised as being inadequate to address spamming and phishing because there is a lack of accountability in Internet systems.[105]

The following legislation has been introduced in the United States to tackle phishing:

The Computer Fraud and Abuse Act (CFAA)

This is regarded as the first federal computer crime statute. It was intended to address the growing threat posed by computer hackers.[106] Section 1030 of the CFAA protects against various crimes involving 'protected computers'. The statute covers any computer attached to the Internet.[107] It prescribes penalties for anyone who intentionally accesses a computer without

---

100 See Sullins n 7 above at 410 and Stevenson n 1 above at 11. Also see Anonymous 'Tech companies unite to tackle phishing' at http://www.elaw@legalbrief.co.za (last accessed on 1 February 2012).

101 *Ibid*.

102 *Ibid*.

103 Rubin *et al* n 2 above at 128.

104 There is also a need by management to enforce corporate security policies together with confidentiality requirements in employment contracts to prevent privileged information from falling into the wrong hands. *Ibid*.

105 Sudhir *et al* 'trust-based Internet accountability: Requirements and legal ramifications' April 2010 *Journal of Internet Law* 3–14 at 3. Sudhir *et al* propose that a trust-based accountability model can best address spamming and phishing.

106 Darden 'Definitional vagueness in the CFAA: will cyberbullying cause the Supreme Court to intervene?' (2009–2010) 13 *SMU Science and Technology Law Review* 329–359 at 330.

107 Kim *et al* n 94 above at 460; 463–464.

authorisation or exceeds authorised access. It was amended in 1986 because of its limited success with indictments.[108] Most of the CFAA's violations require either that the individual access a computer 'without authorisation' or by 'exceeding authorised access'. However, the courts have held that the CFAA does not define what constitutes 'without authorisation'.[109] As a result of numerous revisions, the CFFA was expanded to include a civil cause of action and address initial authorisation but exclude the level of access.[110]

Can-Spam Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act)

This Act regulates spam. It sets out requirements for those who send commercial e-mail, sets out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask e-mailers to stop spamming them.[111] Phishing attacks are said to fall under the ambit of the CAN-SPAM Act.[112] Jeffrey Brett Goodin was the first person to be convicted under the Act during January 2007, when he was found guilty of targeting America Online customers in a phishing scam.[113] However, the CAN-SPAM Act is said to be ineffective in combating phishing.[114]

Anti-Phishing Act of 2005

This Act was introduced by Senator Patrick Leahy in the United States Senate on 28 February 2005.[115] The aim of the Act was to criminalise Internet scams that fraudulently obtain personal information by posing as legitimate online businesses.[116] The Act imposes fines and imprisonment for

---

108 Rubin *et al* n 2 at 128.

109 Darden n 106 above at 329.

110 *Id* at 359.

111 Chief Judge Winmill *et al* 'Cybercrime: issues and challenges in the United States' (2010) 7 *Digital Evidence and Electronic Signature Law Review* 19–34 at 26–27.

112 Lynch n 8 above at 275. Also see Almahroos n 8 above at 609. Regarding criminal penalties under the Act, see Kim *et al* n 94 at 464–465.

113 Almahroos n 8 above at 610.

114 It is not an offence to send an unsolicited commercial e-mail where the consumer has the opportunity to state that he or she does not want to receive any further e-mails from the sender. This is problematic. See Black n 8 above at 85.

115 Stevenson n 1 above 3. Also see Black n 8 above at 85 for a discussion about this Act.

116 Ziring n 11 above at 176; Almahroos n 8 above at 612–613 and Sullins n 7 above at 415–416. Also see Stevenson n 1 above at 3–9 for a discussion, analysis and criticism of the Act. The Act was commended for allowing the prosecution of phishers without showing any specific damages to any individual.

five years on a person who fraudulently creates a website and who sends an e–mail message purporting to come from a legitimate business.[117] The Act was criticised for not containing any guidance or allocation of additional resources for its enforcement.[118] It is not surprising that the Bill was not enacted. It has been mooted that legislation that creates incentives to combat phishing may be more effective.[119]

Access Device Fraud Act

Section 1029 of the Act 18 USC, prohibits the fraudulent use of 'access devices' to steal money.[120] Section 1029 has been useful in phishing cases.[121]

Identity theft laws

The Identity Theft Penalty Enhancement Act, 2004 was signed into law by President Bush on July 15, 2004. The Act was aimed at subjecting identity thieves to tougher penalties. It also includes the length of sentences for those who are convicted of conducting phishing scams.[122] Therefore, this Act establishes a new crime, namely, that of aggravated identity theft (using a stolen identity to commit other crimes) that would include phishing. The Identity Theft Enforcement and Restitution Act of 2008 was signed into law by President Bush in 2008. Its aim was to enhance the identity theft laws. The Act applies to online and offline information theft, addresses phishing and identity theft, and authorises restitution to identity theft victims for their time spent recovering from any harm caused by identity theft.[123]

The US Safe Web Act of 2006

The Undertaking Spam, Spyware and Fraud Enforcement with Enforcers Beyond Borders Act (US Spy Web Act) empowers the Federal Trade Commission (FTC) to protect consumers from phishing and other forms of

---

117 *Ibid*. Also see Lynch n 8 above at 298–299 for a discussion about the Act/Bill.

118 Stevenson n 1 above at 4.

119 Almahroos n 8 above at 613.

120 The term 'access device' has been defined as 'any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or any other telecommunication service, equipment, or instrument identifier, or other means of account access that can be sued, alone or in conjunction with another access device, to obtain money, goods, services or any other thing in value, or that can be used to initiate transfer of funds'. Winmill *et al* n 111 above at 26.

121 *Ibid*.

122 For more information about the Act, see Sullins n 7 above at 413–414.

123 See ss 1028 (a)(7) and 1028A (a) of the Act. Also see s 2 which regulates criminal restitution. See Feigelson & Calman n 9 above at 19.

fraud by improving its ability to share information and to conduct joint investigative efforts with foreign law enforcement agencies.[124] The FTC is also empowered to obtain monetary consumer redress in cases involving spyware, spam and Internet fraud.[125]

Phishing laws in some States

States have made a more concerted effort to tackle phishing. Several states in America have passed statutes making phishing a felony since 2005.[126] The aim of these statutes is to simplify the prosecution of phishing cases by prosecutors. In California, an action for fraud is recognised. A victim of a phishing scam had recourse to a fraud action where the victim has suffered injury as a result of the scam.[127] Chapter 33 of the California Business and Professional Code addresses fraudulent and illegal business practices, and it provides a civil remedy to consumers and ISPs who are adversely affected by phishing scams.[128] It is unlawful in terms of Chapter 33 to induce another person to provide identifying information under the misapprehension that the recipient is a known and trusted online business enterprise. Thus, California provides for civil rather than criminal penalties against phishing. The advent of the Anti-Phishing Act of 2005 in California now makes it unlawful for anyone to use the Internet or electronic means to engage in phishing practices. Victims have monetary redress in the amount of $500,000 per violation or the greater actual damage suffered and scammers may be fined up to $2,500 per violation.[129] California is said to be the first state to have passed an anti-phishing law.[130]

The state of Minnesota has criminalised attempted phishing.[131] Other states have authorised their Attorney Generals and ISP operators or trademark owners to sue phishers for actual or statutory damages.[132] States such as Arkansas, Hawaii, Texas and Virginia have passed laws relating to phishing

---

124 Almahroos n 8 above at 610.

125 See s 3 which addresses remedies available to the FTC.

126 Feigelson & Calman n 9 above at 17.

127 Victims have recourse to California identity theft law when they are victims of identity theft and civil remedies for unlawful business acts or practices. For further discussion, see Ziring n 11 above at 175.

128 It also offers courts the discretion to increase the recoverable damages if the defendant has a tendency to violate the statute and courts may also award reasonable cost order to plaintiffs. *Id* at 176–177.

129 Cherry n 8 above at 596.

130 *Ibid*.

131 Feigelson & Calman n 9 above at 17.

132 *Ibid*.

and similar forms of Internet fraud.[133] Arkansas has enacted the Consumer Protection against Computer Spyware Act, which criminalises the installation of spyware and the collection of personally-identifiable information.[134] In Hawaii, an anti-phishing taskforce has been created to consider options to prevent commerce-based crimes in Hawaii.[135] A Texan law allows ISPs, website owners and trademark owners who are adversely affected by phishing scams, to bring actions against a scammer for the greater of actual damages or $100,000.[136] In Virginia, it is a felony for any person other than a police officer to use a computer to obtain any personally-identifying information by trickery or deception.[137] Thus, Virginia has added phishing to its Computer Crimes Act. Both New Mexico and New York have enacted similar statutes during 2005 and 2006 respectively, whilst the state of Washington has criminalised attempted phishing.[138] Connecticut and Louisiana have introduced legislation granting aggrieved individuals the right to seek recovery, whilst Connecticut and Utah have enacted laws that provide criminal penalties for phishing.[139]

The above discussion demonstrates that phishing is being addressed at both state and federal levels in the United States. Many laws have been introduced to combat phishing scams at federal level such as, *inter alia*, the Can-Spam Act of 2003, Access Device Fraud Act, Identity Theft Enforcement and Restitution Act of 2008 and the US Safe Web Act of 2006. These laws have proved to be useful in securing convictions in phishing cases. The provisions addressing monetary consumer redress are commendable as consumers need to be compensated for losses sustained through phishing scams. The roles of law enforcement agencies such as the FBI and the Department of Justice in tackling phishing internationally through international cooperation are also lauded as phishing transcends national boundaries. The collaborative efforts by large tech companies in the United States to combat e-mail scams and phishing demonstrates the active roles of such tech companies in eliminating opportunities for phishing scams. These efforts are regarded as positive steps in the fight against

---

133 Ziring n 11 above at 176.
134 *Ibid*.
135 *Ibid*.
136 *Ibid*.
137 *Ibid*. Also see Black n 8 above at 85.
138 Black n 8 above at 86. Also see Almahroos n 8 above at 618.
139 For a detailed discussion about state legislative efforts, see Almahroos n 8 above at 614–621. Also see Calman n 9 above at 2–5.

phishing. The creation of an anti-phishing task force in Hawaii to address commerce-based crimes is also lauded.

The European Convention on Cyber Crime

The Convention criminalises certain computer actions and it is regarded as the first international treaty on crimes on the Internet.[140] The Convention strives to *inter alia*, achieve unity between member states, foster cooperation between states by adopting a common criminal policy aimed at the protection of cyber crime, and by the adoption of sufficient measures to combat such criminal offences. Notwithstanding the above, the Convention is mindful of the need to ensure a proper balance between the interests of law enforcement, and the respect for fundamental human rights and the need for protection of personal data, as set out in the Preamble. The Convention is considered to be one of the most organised coordinated efforts to fight phishing and related cyber crimes.[141] However, it contains no provision for cooperation in securing computer networks.[142]

South Africa has adopted the Convention but has not ratified it. South Africa needs to ratify the cyber crime treaty to avoid becoming an easy target for international cyber crime such as phishing. Although substantive obligations are in place, South Africa needs to revise some procedural provisions to comply with the treaty such as introducing a 24/7 contact centre.[143]

Law enforcement officials globally are recognising the need to co-operate with another to curtail cross border cyber criminal activity.[144] To illustrate this, cooperation between the US and Romania has resulted in convictions in both countries for criminals who were involved in phishing-related crimes tied to organised crime enterprises worldwide.[145] Similarly, the United Kingdom's National Hi Tech Crime Unit is working with the FBI and the

---

[140] It was signed in Hungary on 23 November 2001. Its aim is to combat cybercrime. See Cassim n 19 above at 126; Kim *et al* n 94 above at 487; Sullins n 7 above at 420–426 for a discussion about the Convention and its impact on the US, see Almahroos n 8 above at 613–614.

[141] Nykodym *et al* n 7 above at 255.

[142] This is problematic. See Brenner & Clarke 'Distributing security: preventing cyber crime' 2005 *John Marshall Journal of Computer and information Law* 659–709 at 671.

[143] Cassim n 19 above at 131.

[144] Sullins n 7 above at 411.

[145] Nykodym *et al* n 7 above at 256.

US Secret Service to investigate phishing attacks in the United Kingdom.[146] The United States acceded to the Convention on 1 January 2007.[147]

The role of the Anti-Phishing Working Group (APWG)

The APWG is a worldwide coalition which unifies the global response to cyber crime across industry, government and law-enforcement sectors.[148] The APWG analyses phishing attacks reported to it via its member company, the Global Research Partners. Its membership comprises more than 2000 global institutions and its directors, managers and research fellows advise national governments, global governance bodies such as ICANN, international trade groups, and multilateral treaty organisations such as *inter alia*, the European Commission, Council of Europe's Convention on Cyber Crime, United Nations Office of Drugs and Crime and the Organisation of American States. The APWG has reported that 2013 was one of the most active years on record for phishing, with the US continuing to be the top country hosting phishing sites during 2013.[149] The APWG phishing attack repository is considered to be the Internet's most comprehensive archive of e-mail fraud and phishing activity.[150] The role of the APWG is commendable.

GUIDELINES FOR SOUTH AFRICA

It is submitted that South Africa can learn from the American experience in addressing phishing. It is noteworthy that both the ECT and POPI do not address the crime of phishing *per se*. However, as phishing involves Internet fraud, it may conceivably fall within the ambit of sections 86 and 87 of the ECT. POPI addresses identity theft which is a form of phishing. However, there is dearth of decided case law on phishing cases in South Africa. In the United States of America, laws such as the Can-Spam Act of 2003 and the Access Device Fraud Act have proved to be useful in securing convictions in phishing cases. Both the Identity Theft Enforcement and Restitution Act

---

146 Sullins n 7 above at 411.

147 Kim *et al* n 94 above at 487. This bodes well for tackling international phishing.

148 Anonymous 'APWG' at: http://www.antiphishing.org/about-APWG/ (last accessed on 17 June 2014).

149 Statistics also indicate that phishing is continuing to rise in China with Chinese phishers victimising the growing online population of the country. Anonymous 'APWG News' at: http://www.antiphishing.org/apwg-news-center/ (last accessed on 17 June 2014).

150 It has been reported that government agencies such as the US and United Kingdom tax authorities and social networking sites such as Facebook, have been attacked by phishers. Nykodym *et al* n 7 above at 254. Also see Black n 8 above at 79 and Cherry n 8 above at 594.

of 2008 and the US Safe Web Act of 2006 contain provisions addressing monetary consumer redress. These provisions also compensate the victim for time spent recovering from the harm suffered as a result of the phishing scam. This is noteworthy as victims should receive compensation not only for financial losses caused by phishing scams. It is submitted that POPI does not contain a similar provision. Law enforcement agencies in South Africa (such as the South African Police and the Hawks) can emulate their American counterparts such as the FBI, the US Secret Service and the Department of Justice by tackling international phishing through international cooperation. South African tech companies can also learn from the approach of American tech companies in addressing phishing scams. South Africa should also investigate the feasibility of creating an anti-phishing task force to address e-commerce crimes. It is submitted that both the United States of America and South Africa have introduced legislation that can be used to combat phishing. However, it is submitted that such legislation can be improved upon. The need arises for more comprehensive legislation to address the spectre of phishing.

CONCLUSION

The above discussion illustrates that it is difficult to deter phishing because it is more expensive than traditional crimes and because of the anonymity of the Internet. The menace of phishing has pervaded all societies. A multifaceted approach is required to curb phishing and greatly reduce its threat and impact on victims. Banks have an obligation to provide their clients with a safe and secure banking environment. Banks need to routinely warn their customers about the perils of phishing and constantly upgrade their security systems to address online scams. If banks fail to meet their obligations to their clients, they can be held liable if their clients fall victim to phishing schemes.[151] In order to avoid liability, banks have to prove negligence on the part of their clients through the failure of clients to take adequate measures to protect themselves from fraudsters.[152] The

---

[151] Clients have to prove that their banks did not take adequate measures to protect them from fraudsters, for example, by the banks failing to detect suspicious activities on their clients' accounts. Also see *Experi-Metal v Comerica* US DC (for the Eastern district of Michigan) Case 09–14890 June 13 2011, where the court held that the bank had failed to discharge the burden of good faith and was thus liable for financial losses suffered by customers as a result of a phishing scheme.

[152] Moodley – Isaacs'Banks must prove that you are negligent' *The Saturday Star* 1 May 2010 at 1. Also see *Roestoff v Cliff Dekker Hofmeyr Inc* (34306/2010)[2011] ZAGPPHC 219 (2012); 2013(1) SA 12 (GNP), where the court held that the attorney's negligence had contributed to his financial loss in a phishing scam.

sophistication of computer attacks together with the complexities of the modern computer age require organisations and banks to remain proactive, and use 'defence in-depth' security measures to stay ahead of such attacks.[153]

Internet users also need to be vigilant when transacting online and they must avoid becoming victims to phishing operators. Consumers should use banks that have increased security measures, be cyber smart and ensure protection online. Internet users should not open e-mails, click on attachments or respond to messages which are not familiar as phishers often bait computer users by sending e-mail requests that appear to be from legitimate financial organisations.[154] Users should also check the legitimacy of e-mails by contacting the financial institutions. Customers should be aware that banks will never send e-mails with links requesting clients to verify their details.

A close partnership between law enforcement agencies and the private sector is also necessary to address bank-related crime and to ensure that cyber crime such as phishing, is not allowed to thrive in the country. It is important to maintain consumer confidence in online commerce. The most effective way to protect consumers from phishing scams is to educate them so that they will not be deceived by the online fraudsters.[155] Phishers are exploiting weaknesses in the current state of technology. Therefore, the focus should be on technological changes with legislation playing a supporting role.[156] Consumer awareness should be utilised together with technological improvements to address the phishing problem. Internet-industry groups and technology companies should also play a pivotal role in making the Internet safer and more secure for consumers and restore consumer confidence. While organisations such as software manufacturers, ISPs and the credit industry can introduce spam or phishing filters and firewalls to screen incoming e-mails, they should also keep up to date with advancing technology to counteract potential threats to IT security. Thus far, phishers have been able to exploit weaknesses in the preventative measures introduced by businesses and computer technology organisations.[157]

---

153 The phrase 'defence in depth' security measures refers to the process whereby companies continuously improve their methods of defences in multiple layers in order to avert potential threats. Such measures involve the use of monitoring systems to detect suspicious network activities. For further discussion, see Reach n 24 above at 12.

154 See Pierson n 39 above at 24, Reach n 24 above at 13 and Vittal n 7 above at 2.

155 Ziring n 11 above at 178. Also see Lynch n 8 above at 276, 278.

156 Stevenson n 1 above at 3.

157 *Id* at 10.

However, such organisations should make a concerted effort to terminate active phishing sites, incorporate consumer education and on-going policing efforts to prevent phishing attacks from occurring. They should fight phishing via technology and look for effective solutions to benefit phishing victims.[158] Thus, it may be necessary to fight technology with technology.[159]

Organisations should also make phishing awareness a necessary part of employee training and development to counteract such crime.[160] They should take such measures because they have a vested interest in counteracting phishing attacks. It has been mooted that ISPs should become liable for the actions of phishers because they provide phishers with e–mail access and web space.[161] The introduction of secondary liability on ISPs through legislation could provide the much needed boost for such operators to take a more active role in fighting phishing.[162] Law enforcement agencies who are involved in the investigation and prosecution of cases should be technically savvy and receive adequate technical training and education to fight such cyber crimes. Many criminals send phishing scams from overseas, which causes jurisdictional difficulties in the investigation and prosecution of such crimes. Therefore, domestic legislation is not the only method to combat phishing, but international cooperation between countries and law enforcement agencies is also required to investigate and prosecute cyber crime, such as phishing.

The role of the Anti-Phishing Working Group in finding solutions to the phishing problem is commended. Although attempts by the United States of America and South Africa to address phishing are encouraging, more is needed. The introduction of more comprehensive legislation to address the spectre of phishing in South Africa is advocated. Such legislation should address the following aspects:

- the crime of phishing specifically;
- introduce stringent penalties for phishing scams or attacks ranging from fines and imprisonment for five years to fines for R10 million or

---

158 For a discussion about the measures to be taken by software manufacturers, ISPs and the credit industry, see Lynch n 8 above at 286–292. Also see Black n 8 above at 91.

159 Nuth n 1 above at 446.

160 Nykodym *et al* n 7 above at 256.

161 This would result in ISPs being held liable for the actions of third parties, thereby resulting in secondary liability being imposed on ISPs. Feigelson & Calman n 9 above at 20.

162 Calman n 9 above at 23–24.

imprisonment for 10 years, depending on the severity of the offence and the status of the online fraudster (considers whether the fraudster is acting alone or is part of an organised criminal syndicate);
- jurisdictional hurdles facing countries (such as South Africa) as a result of phishing being a cross-border crime;
- encompass extradition provisions because of the international nature of phishing;
- include remedies for restitution to victims of phishing scams (similar to the provision in the Identity Theft Enforcement and Restitution Act of 2008 in the United States of America);
- a provision on international cooperation, sharing of information and the conduct of joint investigative efforts with foreign law enforcement agencies (similar to the US Safe Web Act of 2006);
- include a provision on training and skills development for law enforcement agencies, the prosecution and the judiciary to make their personnel more technically knowledgeable (it is submitted that this would apply more to developing countries such as South Africa);
- Guidance on the allocation of resources for the enforcement of such legislation (to avoid similar criticisms which were levelled at the Anti-Phishing Act of 2005 in the United States of America);
- the introduction of secondary liability on ISPs, tech companies and financial institutions to ensure that such organisations adopt more substantial anti-phishing measures; and
- ensure a proper balance between the interests of law enforcement, and the respect for fundamental human rights and the need for protection of personal information (in line with the European Convention on Cybercrime).

As stated earlier, education and awareness by consumers are also important strategies against phishing attacks.[163] Indeed, a collaborative effort is needed to unite lawmakers, consumers, industry leaders in technology, banking and financial services to combat phishing.[164] At the end of the day, a multifaceted approach supported by comprehensive legislation, will go a long way towards preserving the positive aspects of the Internet and combatting cyber crimes such as phishing.

---

[163] Lynch n 8 above at 276; 278.
[164] Sullins n 7 above 410.