CYBER SAFETY EDUCATION FOR TEACHERS – COMMUNITY ENGAGEMENT THROUGH ACADEMIC LEARNING

E Kritzinger
University of South Africa
South Africa
kritze@unisa.ac.za

ABSTRACT – We are currently living in a technology-driven world where technology has become part of our daily lives. Information and communication technology (ICT) is used for socialising, business, leisure and education. ICT devices range from laptops and tablets to cell phones, and most of these have access to the internet. With the increase of ICT devices and the decrease in the cost of these devices and internet connectivity, more and more people are becoming ICT users. These users range from business employees to home users. One group of home users also becoming more prominent is school learners. Using ICT devices has many advantages, especially within the education environment. However, there are also a number of disadvantages associated with the use of ICT and ICT devices. Through recent studies it is clear that school learners are not aware of proper and safe use while connected to the internet. This can result in a number of cyber risks which include cyber bullying, identity theft, phishing attacks and social and emotional problems. It is therefore vital that all school learners be properly educated and made aware of cyber risks. The current problem within South African schools is that cyber safety education is not included in the new CAPS curriculum. The second problem is that most teachers do not understand cyber risks and are therefore unable to assist the learners. This research focuses on teachers and the main aim is to assist them in gaining cyber safety knowledge and skills so that they can help their learners become cyber safe. The research proposes an open distance learning (ODL) approach through a cyber safety course offered by an ODL academic institution. This approach will be a six-month distance-based course that will be free for all school teachers. The research investigates the feasibility of this approach to determine the value added in transferring cyber safety knowledge to the community of school teachers.

Keywords: Cyber safety, Awareness, Teaching and learning, Community engagement

1. INTRODUCTION

Information and communication technology (ICT) has become one of the fastest growing technologies across the globe (WolfPack, 2013). We are living in a technological world where all aspects of our daily lives are connected to technology. The use of ICT is growing due to the increasing availability of ICT devices, for example laptops, tablets and cell phones (Labuscagne & Eloff, 2012). Most of these devices have internet access and allow users to be connected 24/7. With the continued increase in the availability of ICT devices and the decrease in the cost of using them, more people are becoming cyber users (Grobler & Dlamini, 2012).

Cyber users can be defined as users that are connected to the internet through an ICT device. They are divided into two groups: cyber users that are within a working environment and home users (Kortjan & Von Solms, 2014; Kritzinger & von Solms, 2010). The research focuses on the second group – home users. One section of home users that are extremely vulnerable to cyber threats is school learners (Jobi & Kritzinger, 2014). School learners do not have the proper knowledge and skills to be connected safely to cyber space. Teachers lack the same knowledge and skills. This research therefore focuses mainly on improving teachers' knowledge and skills of cyber safety. The idea is that if teachers are properly educated, they will be able to assist school learners in gaining the same knowledge and skills to improve their cyber safety awareness.

Why is cyber safety awareness important? The advantages of cyber access are numerous. Cyber access can enrich the lives of cyber users by means of socialising, working and education (WolfPack, 2013). However, with the advantages come disadvantages. There are many cyber risks and threats associated with cyber use, for example identity theft, cyber bullying, phishing attacks and malware (Badenhorst, 2011; WolfPack, 2013). These cyber risks and threats can have a negative impact on users if users do not protect themselves and their information.

This research focuses on improving teachers' cyber safety knowledge and skills with the purpose of growing a cyber safety awareness culture within South Africa. This research is part of a community-engaged learning initiative within the School of Computing, which resides within the College of Science, Engineering and Technology (CSET) at the University of South Africa (Unisa). Unisa is one of the biggest open distance learning (ODL) universities within Africa. The main focus of this research is to enhance community-engaged learning in an attempt to grow a national cyber safety culture in South Africa.

2. COMMUNITY-ENGAGED LEARNING IN SOUTH AFRICA

Community-engaged learning is not a new concept. The concept was first mentioned in the Education White Paper 3: A Programme for the Transformation of Higher Education within South Africa (Department of Education, 1997). The White Paper clearly stated that universities had to be proactively involved in community development. However, over time this mandate has been implemented more theoretically than practically. This issue is readdressed within the 2014 White Paper.

The new White Paper for Post-School Education and Training by the Department of Higher Education and Training in South Africa was published in 2014. The document clearly states that the concept of *community engagement and graduate community service* should no longer be only a theoretical idea, but should be practically integrated and implemented to the advantage of communities (Department of Higher Education and Training, 2014). The document continues and clearly states: "The issue of community engagement and graduate community service remains a complex issue because it pertains to many different areas of university and academic work. What has emerged is that community engagement, in its various forms – socially responsive research, partnerships with civil society organisations, formal learning programmes that engage students in community work as a formal part of their academic programmes, and many other formal and informal aspects of academic work – has become a part of the work of universities in South Africa." This indicates that it is a compulsory mandate for all higher education institutions to ensure that community engagement is implemented practically to the advantage of the community. This research contributes to community engagement within Unisa, focusing on cyber safety awareness for cyber users (teachers).

2.1 Unisa

Unisa has committed itself to community-engaged learning. This commitment is clearly shown in that Unisa invested more than R35 million in 227 community-based projects in 2013. This relates to 3 621 164 hours of community engagement and outreach projects for different communities (University of South Africa, 2014). In this way the institution is ensuring that academics dedicate a certain portion of their time to community engagement. However, it is important to note that community engagement projects are not yet community-engaged learning by nature. Some kind of tuition (teaching and learning) must take place to ensure that this is in line with the vision and mission of improving community-engaged learning. It is therefore vital for community engagement projects to grow over time to include a tuition aspect that ultimately contributes to the knowledge sharing that will uplift communities.

2.2 School of Computing

The School of Computing in CSET has a number of community engagement projects in place already. One of these projects which have contributed to communities over the last five years is the Cyber Safety Awareness and Education Project. The project has been involved in proactively contributing to growing a cyber safety culture amongst school learners and school teachers. The project is ready to start including tuition as the first step to becoming a community-engaged learning project.

The School of Computing currently has five information security modules/courses. These courses are divided into formal and centre courses.

Formal modules are part of a qualification. Participants can only enrol for these modules if they are enrolled for a qualification at Unisa. The information security modules within the School of Computing consist of two information security courses (INF4831 and CPS401l). Both of these courses are NQF level 7, relating to honours modules. These modules are therefore not suitable for a community-engaged learning project as they are part of a formal qualification.

The second group of information security modules/courses is within the school's short learning programme centre, the Centre for Software Engineering (CENSE). The modules offered within the centre are mostly six-month courses (based on the semester timeline). These are standalone courses and do not form part of a qualification. The three existing information security courses are the following:

- CSIS1DF (NQF level 5) – Introduction to Information Security
- CSIS02D (NQF level 6) – Applied Information Security
- CSIS03D (NQF level 7) - Advanced Information Security

The average fee for a short course is about R4 500 (this includes the textbook and study material). These three courses are not viable for community-engaged learning due to the cost and the prerequisites. The research focuses on a possible community-engaged learning opportunity that will have no cost to the participants. A free short course in cyber safety awareness that can be offered to the community is investigated.

3. INTEGRATED APPROACH TO SCIENCE AND TECHNOLOGY

The integrated approach is not a new concept and has been successfully implemented at Unisa (see section 2). Within CSET, the concept of community-engaged learning is still very new. Currently within the CSET there is still a silo approach to research, tuition (teaching and learning) and community engagement. One of the main reason for this is that technology based knowledge (for example programming) is not as easy to translate into integration as social related knowledge (for example ensuring food supplies). The results are that CSET have limited integration currently between tuition, research and community engagement.

In this paper an integrated approach is proposed for tuition, community engagement and research within a community-engaged learning course for the School of Computing, CSET. The aim of the proposed integration approach is to show integration in technology subjects is viable. The approach will includes creating and implementing a course that will focus on teacher education to improve their cyber safety knowledge and skills. Figure 1 depicts the different building blocks that will be included in the planning of this course.

Figure 1: Building blocks for community-engaged learning course

Each of the building blocks depicted in figure 1 will be examined separately in the next sections. It is important to note that all building blocks must be in place and interacting to ensure community-engaged learning.

3.1 Funding

Funding is one of the most important aspects when proposing a free community-based tuition approach. This approach will incorporate two funding options. The first option is funding through the university by means of existing community projects. The second funding option is through industry sponsors. The Cyber Safety Awareness and Education Community Project has budgeted for R100 000 to use as seed money for the project, and this will include material design, admission fees and university overheads. The project aims to obtain additional funding through industry sponsors.

3.2 Tuition

The second building block is tuition - teaching and learning. This building block is the core function of the university and will be the main driver to ensure that participants in this course gain the necessary knowledge to enhance their cyber safety awareness. The tuition material will be divided into ten sections that cover relevant aspects related to cyber safety. Each section will be assessed and a pre- and post-assessment will take place to assess the level of learning. This process will be explained in more detail later in this paper. The assessment levels will be set according to Unisa policies. All participants that pass the set assessments will obtain a certificate under the Unisa name.

3.3 Knowledge transfer

One important aim of this course is that the knowledge that participants gain from the course must be transferred to the school learners within their school environment. The participants will obtain teaching material at the end of the course that will assist them in teaching cyber safety to their school learners. Figure 2 depicts the process of teaching and learning, transferring information to knowledge and lastly knowledge sharing with the community.

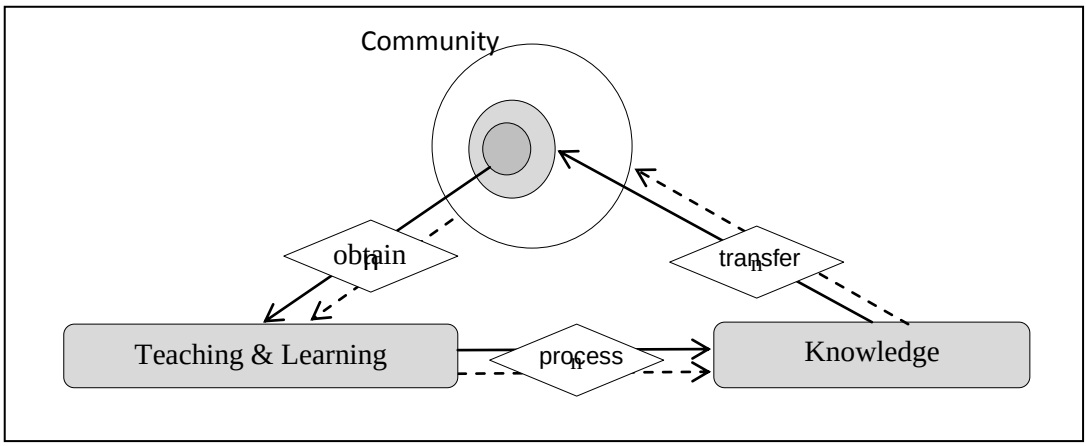

Figure 2: Knowledge process and transfer

In figure 2 the largest circle represents a community. The first inner circle represents school learners and the smallest circle represents the school teachers. The solid arrow line indicates the current aim of the project to ensure that knowledge is transferred to school learners. If the project is a success, this knowledge transfer can be to the wider community (indicated by the broken arrow line).

At the start of this project, the community will include only teachers, i.e. high school and primary school teachers. If enough funding is obtained by either the university or from industry, the project can be opened up to any adult. This will be the long-term plan due to the fact that parents are also in dire need of cyber safety education.

3.4 Research

One main pillar in the academic environment is research (University of South Africa, 2012). The integration between tuition, community engagement and research is now one of the university's main focuses. Within the 227 registered community engagement projects at Unisa, only 40 accredited articles were published and only 80 non-accredited outputs were achieved (University of South Africa, 2014). In other words, there was an average of one accredited output per 22 projects and one non-accredited output per 2.8 projects (University of South Africa, 2014). It is therefore important that more research be generated from projects. This project will be ideal to use as a research basis. The participants will be tested to determine their existing knowledge and skills by means of a questionnaire administered before the course starts. The same questionnaire will be completed again by the participants after the course. The data obtained before and after the teaching and learning will indicate if the course has contributed to developing cyber safety knowledge amongst the participants.

4. NEW PROPOSED COMMUNITY ENGAGEMENT COURSE: CYBER SAFETY EDUCATION

The main focus of the new community engagement tuition course will be cyber safety awareness. The main participants (first intake) will be teachers. The course will consist of learning material and online integration.

There will be four assessments within this course. The first assessment will be the pre-testing. The second and third assessments will be an assignment and the fourth assessment will be the exam testing.

- The first assessment will not count any marks, but will be compulsory.
- The second assessment will count 50% towards the year mark and will be compulsory.
- The third assessment will count 50% towards the year mark and will be compulsory.
- The fourth assessment will count 100% and will contribute 80% towards the final mark.

The final assessment will be used as the post-research component to compare with the first assessment, the pre-test. It will include some of the pre-test questions but new questions as well. All assessments will be in the form of multiple-choice questions.

Outcomes of this project aim to:

- Increase cyber safety knowledge of teachers
- Course material designed for teachers
- Accessible to all teachers (no cost involve)
- Increase research outputs relating to teacher awareness regarding cyber safety
- Knowledge transfer back into the community / school learners
- Providing supporting material for teachers for proper knowledge transfer to take place

5. SUPPORT MATERIAL FOR THE SCHOOL LEARNERS

The course will provide free support material for the teachers to use when teaching cyber safety to the school learners. This material will cover all the topics that were dealt with on the course. This will provide the teachers with the proper knowledge and skills to assist school learners. The material will include a cyber safety pledge, posters, workbooks and activity books.

Some examples of the support materials are depicted in figure 3.

Figure 3: Free support materials

Workbooks are available in English and have been translated into isiZulu, Afrikaans and Sesotho. If additional funding is obtained, translation into more languages will be possible. The material will be available on the course website to download as needed by the teachers. The workbooks have content relating to different cyber aspects, discussions sections and activities.

6. CONCLUSION

ICT and ICT devices are part of our daily lives. Technology is becoming more available and at a lower cost. The result is that more and more users are using ICT devices daily. ICT has numerous advantages if used properly and these are related to education, socialising, information gathering and work. However, just as many risks and threats are associated with ICT use, for example identity theft, phishing, loss of money and personal information. It is therefore vital that all ICT users be made properly aware of possible cyber risks and threats. This research focuses mainly on school teachers to acquire cyber safety knowledge and skills, which could then be transferred to school learners at the teachers' schools. The research proposes that this can be achieved through community-engaged learning at Unisa, by means of a free online course.

7. REFERENCES

Badenhorst, C. (2011). Legal responses to cyber bullying and sexting in South Africa. *Centre for Justice and Crime Prevention*. Retrieved from http://www.cjcp.org.za/articlesPDF/32/Issue Paper 10-1.pdf

Department of Education. (1997). *Education White Paper 3: A programme for the transformation of Higher Education*. *Pretoria: Department of Education*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Education+White+Paper+3:+A+programme+for+the+transformation+of+Higher+Education#3

Department of Higher Education and Training. (2014). *Post-School Education and Training White Paper for Post-School Education and*. Retrieved from http://www.dhet.gov.za/SiteAssets/Latest News/White paper for post-school education and training.pdf

Grobler, M., & Dlamini, Z. (2012). Global Cyber Trends a South African Reality. In *IST-Africa 2012 Conference Proceedings* (pp. 1–8).

Jobi, T., & Kritzinger, E. (2014). Online Awareness among Sepedi School Children in South Africa. In *Proceedings of the Ireland International Conference on Education (IICE-2014)*.

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *SACJ*, (52), 29–41.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. doi:10.1016/j.cose.2010.08.001

Labuscagne, W., & Eloff, M. (2012). The effictiveness of online gaming as part of a security awareness program, *2010*.

University of South Africa. (2012). Research and innovation policy 1 1. Retrieved from http://www.unisa.ac.za/cmsys/staff/contents/departments/tuition_policies/docs/Curriculum Policy - appr Council - 19 11 2010 - rev appr Council - 23.11.2012.pdf

University of South Africa. (2014). *UnisaWise 2014*. Retrieved from http://www.unisa.ac.za/happening/docs/UnisaWise_Summer2014.pdf

WolfPack. (2013). *201/2013 The South African Cyber Threat Barometer.* Retrieved from http://www.wolfpackrisk.com/wp-content/uploads/2012/10/SA 2012 Cyber Threat Barometer_Medium_res.pdf