Online safety in South Africa – a cause for growing concern

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

***Abstract* - We live in a technology-driven world, where information communication technology (ICT) is increasingly affordable, obtainable and accessible to all technology users, especially to school learners. Information communication technologies (ICTs) include a wide range of devices such as mobile phones, internet access, tablets and desktops. More and more school learners are exposed to ICT devices at school, at home and among friends. Besides being used for social purposes, these devices greatly assist school learners with education. However, a number of disadvantages in the form of risks and threats also prevail if learners do not protect themselves and their personal information. ICT or online risks are a cause for growing concern, and awareness and education are urgently required to ensure that school learners understand the risks and threats and how to avoid them. A number of countries have already started to focus on online safety, but South Africa is numbered among those that are falling behind. This paper investigates the current online safety situation of high school learners in South Africa. A number of short- and long-term initiatives are proposed for incorporating online safety into the school environment in an effort to improve online safety among school learners in South Africa.**

Keywords- online, safety, cyber, school leaners, awareness

I. INTRODUCTION

Millions of people throughout the world use different forms of information communication technologies (ICTs) daily [1]. Two key technological advancements to have emerged in the past decade are mobile devices and the internet [2]. Mobile communication and internet access are crucial to the lives of many cyber users and over the past few years the users of these ICT tools have expanded to include children (school learners). School learners utilise their mobile phones and internet access for socialising, education and knowledge gathering, and also out of pure curiosity [3,4].

The benefits of access to mobile communication and the internet are enormous, and this access must be promoted in a proper and safe manner. However, dependence on and use of these ICT tools pose new and dangerous cybersecurity risks and threats [5]. It is therefore essential that all cyber users, especially school learners, understand the online safety risks and threats associated with using the internet and mobile phones [6]. School learners are becoming increasingly at risk when using ICT tools, and are vulnerable to the danger of revealing compromising personal information or being exposed to inappropriate material online. Online users must understand that they are ultimately responsible for their own safety in an online environment [7]. Online dangers associated with mobile and online activities include the following [8]:

- Cyberbullying
- Identity theft
- Access to inappropriate material
- Stalking
- Viruses and malware

In most instances there are no boundaries when school learners connect to the internet or use their mobile devices. Without proper knowledge and supervision, they could therefore access inappropriate material or unwittingly compromise their personal information. It is therefore vital that school learners be educated about all the possible online risks and how to protect themselves. It is also important to educate teachers, parents and caregivers to ensure that they are also aware of the risks, as they need to assist children in this regard.

In a number of countries, online safety receives serious attention and plans have been introduced to educate school learners.

- The government of the United Kingdom (UK) made a deliberate decision to educate school learners aged 11 to 14 about cybersecurity [6]. According to the report entitled Cyber Security Skills: Business Perspectives and Government's Next Steps, teachers will receive training to enable them to teach pupils about cybersecurity [9]. Teaching teachers about cybersafety is one step closer to ensuring cybersafety among school learners; in fact, the topic of online safety has already been formally included in school curricula in many European countries [10].
- Australia is also proactively implementing cybersafety measures, and the Australian government is focusing on educating parents and teachers in an endeavour to protect children online. A number of measures have been implemented to protect Australian children [11].

Unfortunately no similar measures have been taken or are currently being introduced in South Africa [12], and the fact is that online crime and awareness have been largely ignored in this country [13]. According to a leading international expert in

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

cybersecurity, Prof SH von Solms from the University of Johannesburg, cybercrime is unregulated by government in South Africa [13]. Online crime should be viewed not only as a technology issue, but also as a human issue [14]. South Africa must develop a culture of cybersafety awareness so that children are properly forewarned and forearmed within a school environment [2].

It is vital to start creating and implementing policies, procedures, measures and initiatives for the education of all online users in South Africa. The research reported on in this article focuses primarily on school learners and their online activities. Moreover, a number of recommendations will be made concerning the incorporation of online awareness and education into the South African school curriculum.

II. Problem Statement, Research Questions and Methodology

This article reports on an investigation of current online activities among high school learners in South Africa. To improve online safety awareness and education among school learners in South Africa, it is vital to obtain and analyse statistical information on the use and the results of online activities by this group. Our research focused primarily on school learners between the ages of 16 and 19 to obtain realistic statistical data regarding cyberbullying.

Answers were sought to the following research questions:

- What are the current online activities among high school learners in South Africa?
- What initiatives can be implemented to improve online safety within South African schools?

The data for this report was collected through a web-based survey comprising both open-ended and forced-choice responses. Participants were sent a web-link to the survey and assured that responses would be anonymous, as no identifying data was being collected. The questionnaire focused on several areas, including respondent demographics; cell phone and internet use; access to inappropriate material; cyberbullying, and perceptions and experiences.

The final sample comprised 503 respondents (of which 278 were male), representing all races across all nine provinces in South Africa. The respondents were high school learners (67% of whom attended government schools) between the ages of 16 and 19, all with access to the internet.

III. Online Activities Engaged in by School Learners

The first part of this section discusses the online activities engaged in by the school learners who participated in the survey. The second part investigates the findings that emerged from the survey with regard to the current cyberbullying situation among school learners.

A. Online Activities

The survey investigated the length of time the learners spent using their mobile phones and connecting to the internet.

- Three out of five respondents (60%) indicated that they spent more than three hours a day on their mobile phones. This included activities such as sending/receiving SMSs, using WhatsApp/BBM and making/receiving calls.
- The time spent connected to the internet was also shown to be very high, with 41% of the respondents spending more than three hours in an average day on the internet. This included activities such as surfing the internet, playing games and visiting chat rooms.

With regard to parental involvement in the learners' online activities, the following emerged from the survey:

- 82% of learners had access to the internet from inside their bedrooms.
- 35% of learners hid their online activities from their parents.
- 15% of learners used their mobile phone during school hours, even if this was against schools rules.
- 61% of learners indicated that parents and teachers did not monitor their internet use.
- In the case of 62% of learners, no parental guidance software was installed to regulate their internet access.
- 63% of learners accessed inappropriate internet material.
- 93% of learners believed that there are possible dangers and threats associated with internet use.

The majority of respondents were most concerned about the possibility of online scams or the compromise of their privacy or personal information. Threats such as exposure to online predators and inappropriate content, computer viruses and internet addiction were identified as key issues associated with internet usage.

Seeing that cyberbullying – a phenomenon that has gained prominence with increasing internet access – was perceived as an online threat by 41% of learners, the next section will investigate cyberbullying in more detail.

B. Cyberbullying

Although only 4% of learners (20 of 503 learners) claimed to have been victims of cyberbullying and 4% remained uncertain, 65% of learners reported that they were aware of cyberbullying incidents in their schools. In addition, 18% of the learners said they had a friend or family member who had been cyberbullied in some way. An interesting fact was that while 8% of respondents admitted that they had previously cyberbullied another person, 14% of the respondents were uncertain. This uncertainty (for both victims and perpetrators) suggests that more clarity and education regarding this phenomenon is required.

The majority of cyberbullying incidents reported during the study had occurred on instant messaging platforms such as BBM, WhatsApp or Mxit, and on Facebook or in chat rooms. Over 90% of learners used their cell phones to access these networks. The opportunity to remain anonymous that is associated with these social platforms and the internet in general supports the results of the study, which showed that the majority of respondents who experienced cyberbullying were victimised by an anonymous individual (42%), or by someone they had met online and did not know personally (37%).

According to our study, perpetrators were also likely to attend the same school as the victim (37%), but were not generally from the victim's home community. These findings suggest that cautious and informed online navigation, as well as cybersecurity awareness education in schools may influence the nature and prevalence of cyberbullying.

Victims of cyberbullying were mostly likely to speak about the incident to their siblings, and were least likely to discuss the incident with their teachers. The majority of those who did not discuss the incident at all indicated that they did not consider the issue sufficiently important to discuss (45%). Others stated that they were too embarrassed to disclose details (37%), did not feel comfortable talking about it (21%), or did not think that talking to anybody would actually help and make a difference (21%). Despite the fact that 32% of these individuals stated that the cyberbullying incident had no impact on their lives, 32% claimed that they had become depressed and started to avoid digital online mediums.

Feedback regarding cyberbullying by the school learners in our study included the following:

- *Someone just sent me threatening messages to my cell phone and later called to scare me more.*
- *I was called by an unidentified caller and he said I must buy airtime and what was I wearing to bed.*
- *They picked on how I looked and said I would never be successful because of my appearance.*

The survey findings showed clearly that cyberbullying and other online activities are indeed having an impact on school learners and their online safety. The next section offers a discussion of different methods by means of which school learners can be made aware of and educated regarding online safety.

IV. Online Safety Initiatives

Ninety per cent of the learners in the survey indicated that there was a need for more education relating to the prevention of cyberbullying. Furthermore, 46% of respondents were in favour of the inclusion of online or cybersecurity awareness in general as part of the school curriculum.

A. Curriculum

The following (verbatim) phrases are quoted from the suggestions made by school learners regarding online/cyber awareness within a school environment:

- *Include lessons of bullying in life orientation*
- *Using the life skills period to give awareness*
- *By educating the learners in life orientation classes*
- *By including it in the Life Orientation curriculum*

The above feedback given by the learners suggests that Life Orientation classes would offer a suitable opportunity to promote online awareness. Life Orientation deals with the holistic development of the learner throughout childhood. The South African Department of Basic Education (DBE) has been highly responsive in terms of incorporating real-world skills into the school curriculum, because the government recognises that there is value in teaching children how to navigate in the 'real world'. Nevertheless, online safety (which is unquestionably a real-world problem) is not at present included in any of the primary or high school curriculums [12].

The findings of our research therefore indicate that there is growing support among school learners for the inclusion of online awareness in the Life Orientation curriculum at school. This would be the responsibility of the government through the DBE. The Life Orientation curriculum is part of the new CAPS (Curriculum Assessment Policy Statements) curriculum that was introduced into the South African education system in 2013. CAPS is a single, comprehensive, and concise policy document for all the subjects listed in the National Curriculum Statement Grades R–12 [15]. Life Orientation modules for the new CAPS curriculum include the following [15]:

Intermediate Phase (Grades 4–6): Ages 10–12

- Development of self
- Health and environmental responsibility
- Social responsibility

Senior Phase (Grades 7–9): Ages 13–15

- Development of self in society
- Health, social and environmental responsibilities
- Constitutional rights and responsibilities
- Physical education
- World of work

FET Phase (Grades 10–12): Ages 16–18

- Development of self in society
- Social and environmental responsibilities
- Democracy and human rights
- Careers and career choices
- Study skills
- Physical education

Currently, no online safety aspects are included in the curriculums of any of the phases mentioned above. The DBE must understand the threat posed by online activities and proactively contribute to the design and implementation of online safety education in schools. Including the latter in the South African school curriculum is the best strategy for improving online safety among school learners. Since this will involve a lengthy process that will take a number of years to complete, online safety education must be recognised as a long-term goal before a suitable curriculum is implemented in schools. The next section investigates various short-term strategies that schools can adopt to enhance online safety.

B. School Initiatives

If schools require immediate intervention to improve online safety, the introduction of short-term online safety initiatives is advisable. Below are some (verbatim) suggestions made by learners:

- *Through a school campaign*
- *Have a lot of talks regarding this (cyber safety), posters and people who have been involved to speak*
- *Call an assembly and get someone who has experience to talk about the matter*
- *Discussions and talks*
- *Bring in experts to talk to the learners*

It is also important to note that online safety should not be dealt with separately, but must instead be incorporated into all aspects of education. According to one of the survey participants, cyber safety must be dealt with “not in isolation but in conjunction with a topic that are (*sic*) being discussed”. This ties in with the notion that education must deal with real-world issues. It would therefore be important to incorporate cybersafety as part of a real-life scenario presented to school learners.

Although short-term initiatives may be a good solution, they can add to the already demanding workload of teachers and result in extra costs in terms of materials and training. It is therefore vital to ensure that any initiatives adopted by schools must take all the constraints (time, money and training of teachers) into consideration.

Government can greatly assist here. While the curriculum is being developed, the DBE can assist schools with short-term intervention by developing online safety awareness materials, training manuals and awareness activities. It is evidently vital to consider the unique South African environment by taking account of the different languages, the different financial situations of schools and learners’ different degrees of ICT exposure. Any intervention should ensure that all schools, no matter which languages they have selected and irrespective of their financial or ICT situation, should benefit from the interim measures that are introduced. In the section below, some possible initiatives are proposed.

C. Suggested Short-term Initiatives for Online/Cybersecurity Awareness

This section will touch on short-term initiatives that were designed within the framework of the research undertaken to support online security in the South African school environment.

1) Posters and Personal Pledges

Posters and pledges (as depicted in Figure 1) are inexpensive methods of conveying the concept of online safety.

There are 11 official languages in South Africa, and the Constitution states that all school learners have the right to receive education in their own language.

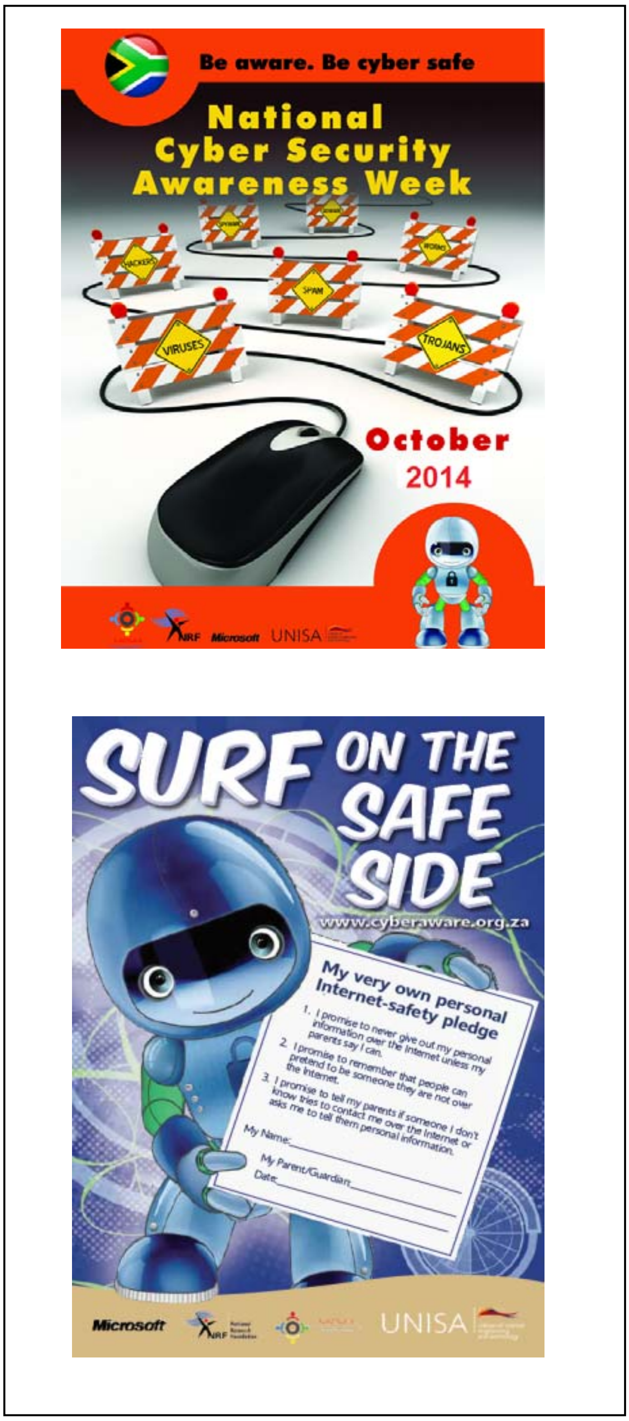
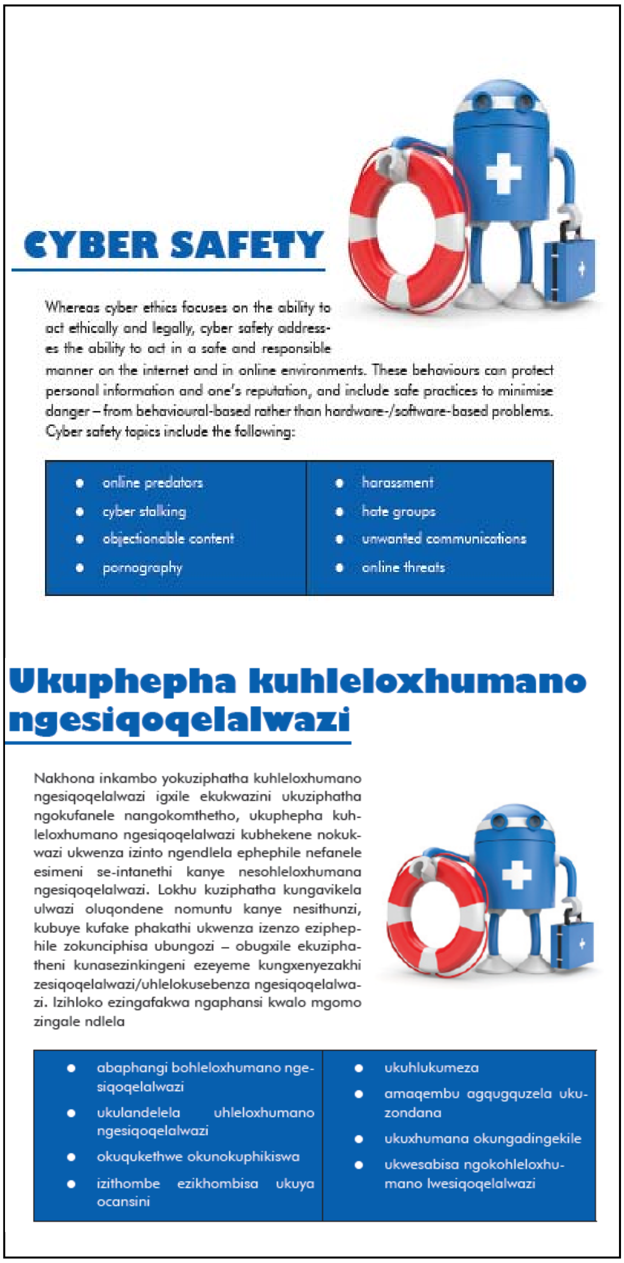

Be aware. Be cyber safe
National Cyber Security Awareness Week
HACKERS
SPAM
VIRUSES
TROJANS
WORMS
October 2014
NRF
Microsoft
UNISA
SURF ON THE SAFE SIDE
www.cyberaware.org.za
My very own personal Internet-safety pledge
1. I promise to never give out my personal information over the Internet unless my parents say I can.
2. I promise to remember that people can pretend to be someone they are not over the Internet.
3. I promise to tell my parents if someone I don't know tries to contact me over the Internet or asks me to tell them personal information.
My Name:
My Parent/Guardian:
Date:
Microsoft
NRF
UNISA

Figure 1: Posters and pledge

It is therefore vital to ensure that all material is made available in all 11 languages. Figure 2 shows posters in English and isiZulu.



CYBER SAFETY

Whereas cyber ethics focuses on the ability to act ethically and legally, cyber safety addresses the ability to act in a safe and responsible manner on the internet and in online environments. These behaviours can protect personal information and one's reputation, and include safe practices to minimise danger – from behavioural-based rather than hardware-/software-based problems. Cyber safety topics include the following:

- online predators
- cyber stalking
- objectionable content
- pornography
- harassment
- hate groups
- unwanted communications
- online threats

Ukuphepha kuhleloxhumano ngesiqoqelalwazi

Nakhona inkambo yokuziphatha kuhleloxhumano ngesiqoqelalwazi igxile ekukwazini ukuziphatha ngokufanele nangokomthetho, ukuphepha kuhleloxhumano ngesiqoqelalwazi kubhekene nokukwazi ukwenza izinto ngendlela ephephile nefanele esimeni se-intanethi kanye nesohleloxhumana ngesiqoqelalwazi. Lokhu kuziphatha kungavikela ulwazi oluqondene nomuntu kanye nesithunzi, kubuye kufake phakathi ukwenza izenzo eziphephile zokunciphisa ubungozi – obugxile ekuziphatheni kunasezinkingeni ezeyeme kungxenyezakhi zesiqoqelalwazi/uhlelokusebenza ngesiqoqelalwazi. Izihloko ezingafakwa ngaphansi kwalo mgomo zingale ndlela

- abaphangi bohleloxhumano ngesiqoqelalwazi
- ukulandelela uhleloxhumano ngesiqoqelalwazi
- okuqukethwe okunokuphikiswa
- izithombe ezikhombisa ukuya ocansini
- ukuhlukumeza
- amaqembu agqugquzela ukuzondana
- ukuxhumana okungadingekile
- ukwesabisa ngokohleloxhumano lwesiqoqelalwazi

Figure 2: Posters in English and isiZulu

Pledges are inexpensive and a pledge form can be supplied to each school learner to sign and take home. This gives learners the opportunity to discuss cybersafety with their parents or caregivers. Growing an online safety culture includes both learners and their parents or guardians. Schools with internet access can download the pledge free of charge and distribute it among learners. However, these initiatives will have greater impact if combined with discussions and worksheets.

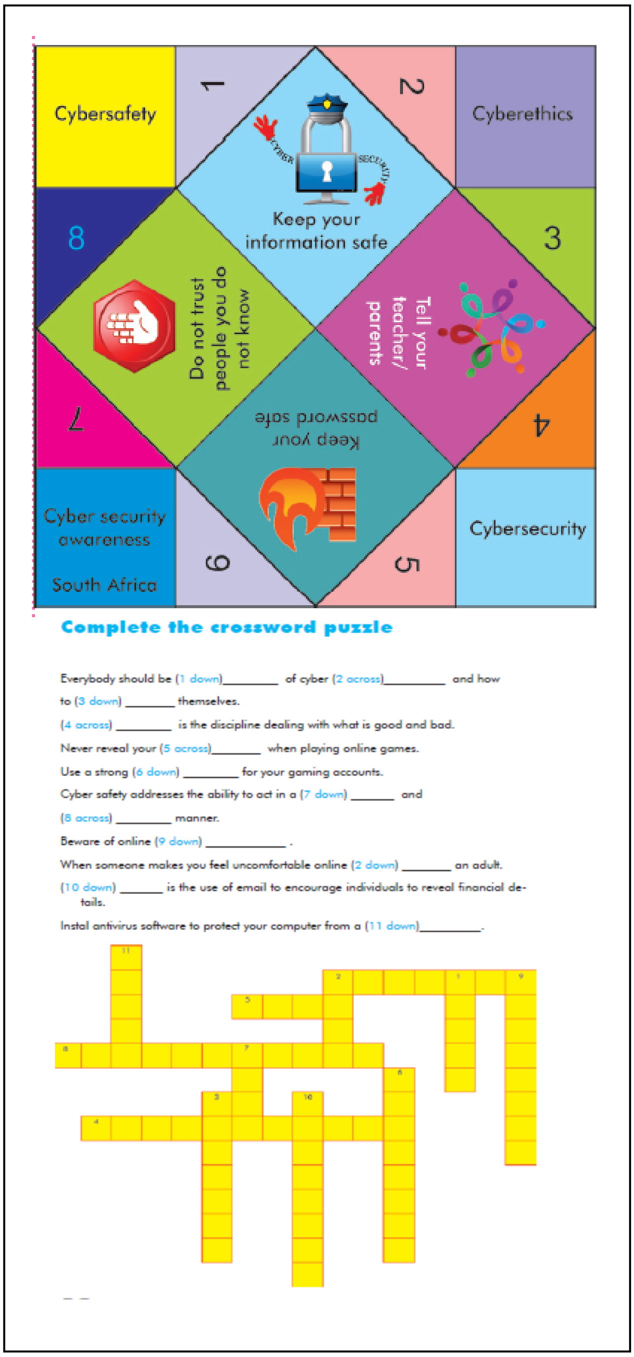
2) Discussions and Workbooks

As part of the research project, workbooks in various South African languages were designed; these included posters, general information and worksheets. The workbooks focused on the different age. Figure 3 depicts the English and Sesotho versions of the workbook.

Figure 3: English and Sesotho versions of the workbook

The workbooks include general information on a number of online safety issues, as well as suggestions that learners can follow to protect themselves against online risks and threats. The workbooks also contain a number of worksheets. Figure 4 depicts two possible activities for different age groups.

All workbook and worksheets that are designed for school leaners must adhere to the new CAPS curriculum. They activities can be used in conjunction with class discussions on relevant online safety issues.



Complete the crossword puzzle

Everybody should be (1 down)_________ of cyber (2 across)__________ and how to (3 down) ________ themselves.

(4 across) _________ is the discipline dealing with what is good and bad.

Never reveal your (5 across)________ when playing online games.

Use a strong (6 down) _________ for your gaming accounts.

Cyber safety addresses the ability to act in a (7 down) _______ and (8 across) _________ manner.

Beware of online (9 down) _____________ .

When someone makes you feel uncomfortable online (2 down) ________ an adult.

(10 down) _______ is the use of email to encourage individuals to reveal financial details.

Instal antivirus software to protect your computer from a (11 down)__________.

Figure 4: Activities for different age groups

3) *Combining Long-term and Short-term Initiatives*

The research reported on in this article investigated the need for both long-term and short-term online safety initiatives to be designed and implemented within a school environment. The main contributor to any online safety initiatives should be the DBE, which should design and implement online safety within the school curriculum and assist with short-term initiatives, as depicted in Figure 5.

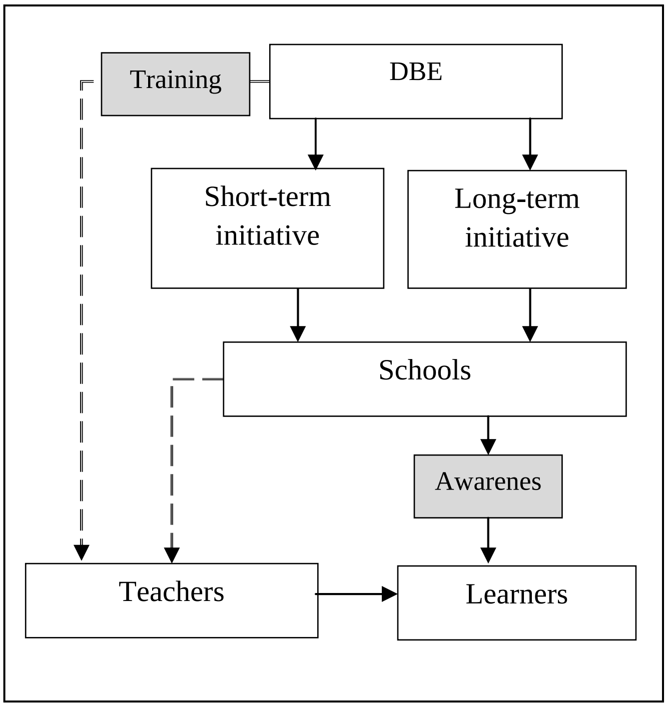


Figure 5: Short-term and long-term initiatives

Figure 5 depicts two possible paths towards enhancing online safety awareness in schools. The first involves the DBE by incorporating online safety awareness in the curriculum. This is seen as a long-term initiative. It is important to note that the DBE must also take responsibility for training teachers regarding online safety and how to engage with school learners about becoming and staying safe online.

The second option is the short-term initiative, which can become the responsibility of either the DBE or of the schools themselves. Short-term initiatives could include awareness strategies such as posters, workbooks, discussions and competitions.

Both short-term and long-term initiatives (school-based and DBE-based respectively) will satisfy the request made by school learners for the greater promotion of online awareness in schools. Teacher training is important not only for long-term initiatives, but for short-term initiatives as well. This online safety awareness will increase online safety among school learners and will contribute to cultivating a healthy online safety culture among all children in South Africa.

V. Conclusion

The research reported on in this article focused on examining the current situation pertaining to online activities and the online safety of high school learners in South Africa. A quantitative approach was used to obtain data from the target group by means of a survey that focused on determining the online activities of high school learners and their position regarding online safety awareness in schools.

The findings of the research were discussed and methods were proposed for incorporating online safety into the school environment. These methods included short-term and long-term online safety initiatives, and it was argued that the main driver of these initiatives should be the DBE, in conjunction with schools. If the DBE and schools start integrating these initiatives in a school environment, the overall online safety of South Africans in general may improve and a culture of cybersecurity awareness may be fostered among all learners.

REFERENCES

[1] Kritzinger, E. & Von Solms, S.H. (2010). Cyber security for home users: a new way of protection through awareness enforcement. *Computers & Security*, 29, 840–847.

[2] Wolfpack Information Risk's report (2012/2013). The South African cyber threat barometer 2012/13. Online available: http://www.wolfpackrisk.com/research/south-african-cyber-threat-barometer/. Accessed on 1 April 2014.

[3] Childnet International (2008). Young people and social networking services: a Childnet International Research Report. Online available: http://www.digizen.org. Accessed on 14 January 2013.

[4] Kriel, L., Kritzinger, E. & Loock, M. (2013). Dangers of using social networks for children online security. Conference proceedings of the 2013 Paris International Academic Conference. ISBN:ISBN:1539-8757

[5] O'Keeffe, G.S., Clarke-Pearson, K. and Council on Communications and Media (2011). *Clinical report – the impact of social media on children, adolescents, and families.* Available online: http://pediatrics.aappublications.org/content/127/4/800.full. Accessed on 1 April 2014.

[6] Farrell, N. (2013). Government to give kids cyber security lessons: new lessons for 11–14 year olds. Online available: http://www.techradar.com/news/software/security-software/government-to-give-kids-cyber-security-lessons-1233480?src=rss&attr=all. Accessed on 20 March 2014.

[7] Furnell, S., Valleria, T. & Phippen, D. (2008). Security beliefs and barriers for novice internet users. *Computers & Security*, 27, 235–240.

[8] Atkinson, S., Furnell, S. & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud and Security, 7*, 13–19.

[9] United Kingdom Government (2014). Cyber security skills: business perspectives and government's next steps. Online available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf. Accessed on 20 March 2014.

[10] Vanderhoven, E., Schellens, T., Valcke, M. & De Koning, E. (2014). Involving parents in school programs about safety on social network sites. *Procedia - Social and Behavioral Sciences*, 112, 428–436.

[11] Australia: Department of Communication (2014). Enhancing online safety for children. Online available: http://www.communications.gov.au/__data/assets/pdf_file/0016/204064/Discussion_Paper_-_Enhancing_Online_Safety_for_Children.pdf. Accessed on 25 March 2014.

[12] Kritzinger, E. & Padayachee, K. (2013). Engendering an e-safety awareness culture within the South African context. Africon 2013. Mauritius. ISBN: 978-1-4673-5940-5. pp. 839–843.

[13] Jones, G. (2014). South Africa neglects alarming effect of cybercrime. Online available: http://www.bdlive.co.za/business/2014/01/14/south-africa-neglects-alarming-effect-of-cybercrime. Accessed on 20 March 2014.

[14] Smith, E., Kritzinger, E., Oosthuizen, H.J. & Von Solms, S.H. (2005). Information security education: bridging the gap between academic institutions and industry. Proceedings of the 4th World Conference on Information Security Education.

[15] Department of Basic Education (2012). Curriculum Assessment Policy Statements (CAPS). Online available: http://www.education.gov.za/Curriculum/CirriculumAssessmentPolicyStatment/. Accessed on 1 April 2013.