SACJ 28(1) July 2016
Research Article

Short-term initiatives for enhancing cyber-safety within South African schools

Elmarie Kritzinger

School of Computing, University of South Africa, South Africa

ABSTRACT
The rate of technological development across the globe is dramatic. The decreasing cost and increasing availability of ICT devices means that its users are no longer exclusively industry or government employees–they are now also home users. Home users integrate ICT in their daily lives for education, socialising and information gathering. However, using ICT is associated with risks and threats, such as identity theft and phishing scams. Most home users of ICT do not have the necessary information technology and Internet skills to protect themselves and their information. School learners, in particular, are not sufficiently educated on how to use technological devices safely, especially in developing countries such as South Africa. The national school curriculum in South Africa currently does not make provision for cyber-safety education, and the availability of supporting material and training for ICT teachers in South Africa is limited, resulting in a lack of knowledge and skills regarding cyber-safety. The research in hand focuses on the situation concerning cyber-safety awareness in schools and has adopted a short-term approach towards cyber-safety among teachers and school learners in South Africa until a formal long-term national approach has been implemented. This study takes a quantitative approach to investigating the current options of teachers to enhance cyber-safety among learners in their schools. The research proposes that short-term initiatives (e.g. posters) can increase learners' awareness of cyber-safety until formal cyber-safety awareness methods have been introduced.

Keywords: cyber-safety, awareness, short-term initiatives, policies

Categories: **Social and professional topics ~ K-12 education**, Social and professional topics ~ Computing literacy, Social and professional topics ~ Human and societal aspects of security and privacy

Email:
Elmarie Kritzinger kritze@unisa.ac.za

Article history:
Received: 14 January 2016
Accepted: 15 March 2016
Available online: 20 July 2016

1 INTRODUCTION

Information and communication technology (ICT) has become an integral part of our daily lives. We use ICT devices for education, information gathering and work-related activities. ICT devices are becoming increasingly accessible to all users due to their greater availability and a decrease in cost. Most of these devices allow users to access the internet. ICT devices and internet access play a particularly important role in the lives of school learners, since technology use is becoming more prominent in the social lives of learners.

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal 28*(1), 1–17. http://dx.doi.org/10.18489/sacj.v28i1.369

SACJ is a publication of the South African Institute of Computer Scientists and Information Technologists. ISSN 1015-7999 (print) ISSN 2313-7835 (online).

The opportunities for socialising and entertainment available to school learners through various ICT devices can be quite beneficial. Recent research has shown that the mobile penetration rate in Africa is increasing, and the majority of school learners nowadays have access to a cell phone (Porter et al., 2015; Wolfpack Information Risk, 2013; De Lange & Von Solms, 2012). However, ICT devices and online access also pose a number of cyber-risks for school learners when they are not educated on how to protect themselves and their information (Furnell, 2010). Cyber-risks include access to inappropriate material, cyber-bullying, identity theft and threats to learners' social and emotional well-being (Byron, 2008; De Lange, 2012). It is essential that all school learners be educated on how to deal with these risks. The question addressed in this research was therefore whether teachers have the required knowledge and skills about cyber-safety to be able to educate and assist their learners. Ensuring cyber-safety within the school environment is a serious internal issue in all countries with internet access (Hanewald, 2008; Perren et al., 2012; Livingstone, Haddon, Vincent, Mascheroni, & Ólafsson, 2014). The issue of enhancing cyber-safety awareness for school learners is overdue and should be addressed (Miles, 2011).

The current research aims to expand the body of knowledge regarding cyber-safety in schools to ensure that school learners are safe when connected to the internet (cyber-environment). The findings are expected to contribute primarily towards understanding the current situation regarding cyber-safety in South African schools. The study investigated the readiness of school teachers to address the level of awareness and education about cyber-safety in their schools. The research proposed a short-term cyber-safety initiative for schools. The approach was afterwards tested within a school environment to assess if cyber-safety knowledge had improved among teachers and school learners.

2 BACKGROUND

Cyber-attacks in South Africa are a growing concern and may result in serious threats to national security (Wolfpack Information Risk, 2013; De Lange & Von Solms, 2012; Kritzinger, 2014). Cyber-attacks are not restricted to a national level and can have an impact on all cyber-users, including school learners, teachers and parents (Byron, 2008). The 2013 Norton cyber-report placed South Africa third on the Norton International list, with 73% of its population having fallen victim to cyber-crime (Symantec, 2013).

Many countries in Africa are ill-equipped to assist school teachers and learners with awareness and education as far as cyber-safety is concerned (Kortjan & Von Solms, 2014). South Africa only began to cultivate a local cyber-safety culture recently (Kortjan & Von Solms, 2012). Information security programmes are a vital instrument in protecting information and other assets (Kruger, Drevin, Flowerday, & Steyn, 2011).

A number of South African companies and organisations have pledged their commitment to the vision of growing a cyber-safety culture (ISC Africa, 2015). Most of the contributions made by these companies and organisations occurred through a website presence aimed at alerting school learners, teachers and parents to the need for an improved cyber-safety culture. The problem is that the contributions are mostly web based and they offer little or no printed material, curriculums or

http://dx.doi.org/10.18489/sacj.v28i1.369

practical training opportunities (S. von Solms & von Solms, 2014). Many cyber-users do not know that they could find information and assistance online. It is obviously a case of 'you do not know what you do not know' and therefore cyber-users are still in the dark regarding the possible risks of cyber-space (ENISA, 2010).

In countries where a limited cyber-safety culture exists, the initial awareness-raising phase must involve more than just a website presence to create awareness among cyber-users and inform them that they can obtain further information, assistance and knowledge (CJCP & UNICEF, 2013).

To date the South African government has not adopted a comprehensive approach to cyber-safety (Kortjan & von Solms, 2012) and the Department of Basic Education does not provide any educational materials on cyber-safety. Teachers and parents are themselves ill-prepared to educate learners about cyber-safety (De Lange & Von Solms, 2012; Govender & Skea, 2015), particularly in the case of the majority of disadvantaged schools in South Africa.

All schools and teachers must be involved in cyber-safety for school learners (Kouttis, 2016). Areas of concern that were identified in the available literature and that should be addressed in promoting a culture of cyber-safety in South Africa include the following:

- Upgrading legislation to improve cyber-safety in South Africa (Grobler & Dlamini, 2012);
- Ensuring the integration between legislation and the implementation of cyber-safety education in schools (Smit, 2015; Badenhorst, 2011);
- Addressing the limited budget and resources allocated to cyber-safety education (S. von Solms & von Solms, 2014);
- Creating and implementing a national cyber-safety awareness plan (Wolfpack Information Risk, 2013);
- Including cyber-safety issues and education in the school curriculum (Kritzinger & Padayachee, 2013; Della Cioppa, O'Neil, & Craig, 2015).
- Creating education and training opportunities for teachers who are generally ill-equipped to understand or to assist with cyber-safety issues (Govender & Skea, 2015; Jobi & Kritzinger, 2014)
- Creating and distributing more printed educational material on cyber-safety to schools to address the lack of available educational material (S. von Solms & von Solms, 2014) and
- Making all material on cyber-safety available in all the official South African languages (Kruger et al., 2011; Mwim & Kritzinger, 2014; Kouadio, 2008).

Based on the literature studied, the research concluded that urgent cyber-safety initiatives must be implemented in South Africa. This study took the above problem areas into account when conducting research on cyber-safety in South African schools. The research focused primarily on the school environment, particularly school teachers and principals, to determine what challenges they faced in addressing cyber-safety of their learners. The aim of the study was to determine whether the problems identified in literature were, in fact, echoed in real life.

http://dx.doi.org/10.18489/sacj.v28i1.369

3 PRE- AND POST-STUDIES AND COLLECTION OF DATA

The current research consisted of two data-collection phases, a pre-study and a post-study. The pre-study was conducted in 2014 and investigated cyber-safety awareness and incidents among school learners by interviewing teachers and principals. The primary focus of the investigation was the current situation in South African schools regarding

- perceptions about cyber-safety issues in schools;
- incidents relating to cyber-safety in schools;
- handling of online/cyber-safety incidents in schools;
- school policies on cyber-safety; and
- teacher approaches towards cyber-safety in the classroom.

The post-study was conducted in 2015 to obtain data on whether a short-term initiative approach was a viable option for increasing cyber-safety awareness in South African schools.

4 CYBER-SAFETY AWARENESS OF TEACHERS IN SOUTH AFRICA

The pre-study focused on obtaining field data to assess the current situation regarding cyber-safety awareness and cyber-safety knowledge of school teachers in South Africa.

4.1 The research instrument

The research adopted a quantitative approach. The interview questions were administered by trained research assistants who used a pre-developed, structured and largely close-ended interview guide. Open-ended questions were included only where deeper description was necessary. The questionnaire focused on several broad areas such as respondent demographics and information, perceptions regarding online risks and threats, understanding and responding to incidents pertaining to cyber-safety, and school policy and education in respect of cyber-safety issues. Ethical clearance was obtained to conduct the study.

4.2 Population and sample

The research was conducted in 169 schools across seven provinces, and 250 teachers and 29 principals were interviewed.

In South Africa, the Living Standards Measure (LSM) is a segmentation tool that is used to understand the market on the basis of access to services and durables, and it serves as a geographic indicator and determinant of standard of living. The “lower LSM” schools in this sample represented the emerging market, while the “higher LSM” schools represented the established market. The final

http://dx.doi.org/10.18489/sacj.v28i1.369

sample included 279 respondents who represented all races in LSM 6âĂŞ10 schools (both primary and high schools were included).

Figure 1 depicts the LSM and educational split for the respondents.

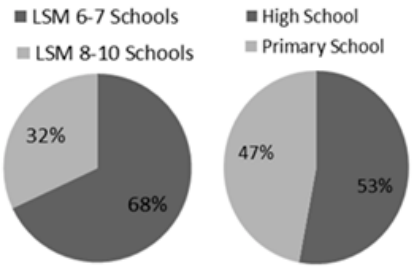

Figure 1: LSM and educational split for the respondents

4.3 Data collection

Data collection was conducted in 2014. Seventeen of the schools in the sample (across Gauteng, KwaZulu-Natal and the Western Cape) were visited for face-to-face interviews, while telephonic interviews were conducted with the teachers and principals from the remaining regions. The post-study was conducted in 2015 to evaluate the proposed short-term cyber-safety initiative within schools.

4.4 Findings and presentation of the pre-study

The data was interpreted and presented in the following order: school policies, perceptions, incidents and learner education.

Each of the above cyber-safety issues was discussed based on an analysis and interpretation of the data collected. The data was kept anonymous to protect the identities of the schools and teachers, as had been agreed when ethical clearance was obtained for the research.

4.4.1 Cyber-safety issues: school policies

In the pre-study, only 56% of all schools indicated that they had a formal cyber-safety policy in place, a finding that was more prevalent among higher LSM schools. Among the lower LSM schools, 34% indicated that they did not have a formal policy and that the introduction of such a policy had never been discussed.

The policies that did exist primarily involved restrictions regarding learners cell phones and internet use when they were at school. Learners were not allowed to use their phones, tablets or other devices with an internet connection–school policy dictated that these devices should be confiscated if they were used in class. However, according to the teachers and principals, learners

http://dx.doi.org/10.18489/sacj.v28i1.369

continued to use their phones and to access the internet during school hours and in class, despite these regulations. The results regarding the existence of school policies on cyber-safety are presented in Table 1.

Other policies and procedures included security settings for controlled internet access, blocking sites such as Facebook and YouTube and pornographic content. A small minority of schools, mostly higher LSM schools, also included guidelines on cyber-bullying in their school rules and regulations relating to bullying in general. Since a policy must be enforced to have value, it is important to note that if a school has a policy that is not properly implemented, enforced and monitored, the policy cannot add value and will not have an impact on improving cyber-safety.

Table 1: School policies on cyber-safety

"Our school ..."	All (%)	Lower LSM (%)	Higher LSM (%)
"...does not have a formal cyber-safety policy and it has never been discussed."	26	34	19
"...does not have a formal policy, but it has been discussed."	15	15	15
"...has a formal policy, but it is not enforced."	3	6	0
"...has a formal policy and it is enforced."	56	45	66

The study revealed that no clear formal policy relating to the handling of cyber-safety incidents that could occur among learners was in place. Teachers and principals indicated that they would prefer policies and regulations to be standardised by the Department of Basic Education before being prescribed to schools. This was largely due to the fact that many schools (especially lower LSM schools) did not have the knowledge, skills or expertise to create a cyber-safety policy on their own. The teachers also argued that if these regulations were issued by the Department of Basic Education, it would be easier for them as school managers to implement and enforce them, seeing that the regulations would not be considered a school requirement, but a government requirement.

To conclude, this section identified that teachers and principals recognise the importance of implementing and enforcing an ICT policy that deals with cyber-safety awareness within the school environment.

4.4.2 Cyber-safety issues: perceptions

The results of this section indicate that 88% of the respondents agreed that learners were exposed to various potential dangers when using the internet. Both teachers and principals (95%) were found to be concerned about cyber-safety issues among their learners. Principals and teachers were also aware that cyber-safety activities/actions could result in threats and risks, and they identified the following threats and risks (see Table 2) in the school environment.

According to Table 2, exposure to and viewing of "inappropriate" content was considered to be the most serious online risk to learners, as pornographic material is increasingly accessible and available through various online mediums. Teachers and principals rated cyber-bullying as the second most distressing online risk to learners. Issues such as the compromise of personal information and exposure to online predators were also flagged as potential issues that posed real dangers to learners within cyber-space.

Table 2: Cyber-risks

	Very serious (%)	Kind of serious (%)	Not serious at all (%)
Learners may see inappropriate content	86	10	4
Cyber-bullying	77	17	6
Learners may be exposed to online predators	76	17	7
Someone can access a learner's personal information	69	16	14
Inappropriate communication with other learners	65	21	15
Online scams	65	24	12
Internet addiction	64	26	10
Viruses	48	28	24
Inappropriate communication with teachers	43	21	36

A total of 81% of the teachers and principals were worried about the impact that online threats may have on learners, confirming that teachers and principals were concerned about cyber-threats and cyber-risks to their learners. Lastly, overall cyber-safety concerns were higher in higher LSM schools than in lower LSM schools.

4.4.3 Cyber-safety issues: incidents

Almost a third (30%) of the participating teachers and principals indicated that they knew of incidents relating to cyber-safety that had occurred among their learners. Once again, this figure was higher in the higher LSM schools.

In the majority of these cases (67%), the teachers and principals had been alerted to the incidents through rumours going around in the school. However, it was found that 55% of the victims had actually reported their cyber-safety case to the school.

Most incidents involved the accessing, viewing and/or sharing of inappropriate pornographic content, followed by instances relating to insulting social media messages and posts. Other issues reported by respondents included cheating in exams using an online source, dangerous meetings resulting from social media experiences, the recording and sharing of 'fight' clips, threatening social

media exchanges and the degrading of schools and teachers in the digital space. Some of these cases had a very serious outcome–in one instance, cyber-bullying had led to the self-mutilation and eventual suicide of the victim. In another instance it had resulted in physical harm to a school learner. Teachers also reported high levels of distress among learners involved in incidents of cyber-bullying.

An alarming 71% of the teachers and principals were of the opinion that although incidents relating to cyber-safety had actually occurred among learners, they had not been reported. One reason for this was that many of the schools did not have processes in place for dealing with cyber-safety incidents so as to assist learners. The teachers and principals also indicated that they believed that learners did not report cyber-safety incidents because there was no process in place to assist them, and because learners were not convinced that teachers could assist them in solving their problems. In fact, 66% of the teachers and principals felt that they were ill-equipped to respond suitably to cyber-safety incidents, which confirms the lack of knowledge and skills about cyber-safety among teachers and principals.

4.4.4 Cyber-safety issues: learner education

More than half of the teachers admitted that they had not provided any information about cyber-safety to their learners, which implies that only about 45% of the teachers had provided their learners with any cyber-safety related information. The primary reason for this was that the teachers did not feel properly equipped to understand and deal with cyber-safety issues.

Furthermore, only 15% of the respondents felt that learners themselves were adequately equipped to deal with the dangers associated with digital space. This finding confirmed the need for cyber-safety education, for which the necessary skills and materials were lacking.

The Department of Basic Education was found to have provided once off cyber-safety training opportunities (for example conferences) to only 21% of the schools in this sample (higher LSM schools–18%; lower LSM schools–25%), whereas 93% of the schools would have liked to receive such material. Furthermore, 34% of the higher LSM schools had received training and support internally (from the school itself), compared to only 5% of lower LSM schools.

The type of training/other support that the schools had received included pamphlets, posters and documents containing guidelines on internet and cell phone use, as well as materials used in Life Orientation classes and in computer labs.

Some of the schools reported that they had held workshops to educate their staff on issues relating to cyber-safety. Schools that had received support from the Department of Basic Education also reported participating in training workshops, as well as receiving pamphlets, emails, newsletters and posters. Despite these contributions, 98% of the respondents felt that cyber-safety should be included in the curriculum. Altogether 92% of the teachers/principals also indicated that they would like to receive training on cyber-safety so that they would be able to competently assist learners, while 96% indicated that they would welcome any initiative or campaign focusing on cyber-safety issues in their schools.

http://dx.doi.org/10.18489/sacj.v28i1.369

5 DISCUSSION AND PROPOSED SOLUTION

This research highlights the concerns of teachers and principals regarding the knowledge and skills of school learners in respect of cyber-space. Although teachers and principals understood the possible impact of cyber-safety incidents on their learners, they lacked the knowledge and skills to assist learners when such incidents occurred. The majority of teachers and principals did not feel adequately prepared to handle cyber-safety incidents, and yet teachers found themselves in a position where they were the primary persons responsible for addressing such issues. From the research it emerged that 90% of the teachers and principals believed that more education was needed in respect of cyber-safety. Teachers and principals therefore agreed that they should be properly equipped to handle incidents relating to cyber-safety if and when they occur.

Despite teachers' and parents' concerns about the cyber-safety of learners, the majority of lower LSM schools and nearly 40% of higher LSM schools did not have a formal policy on cyber-safety. Neither the Department of Basic Education, nor the schools themselves provided sufficient and necessary information to the teachers, and consequently only 28% of learners were receiving enough information on cyber-safety.

The above findings support research that suggests that further education on cyber-safety is necessary to control incident rates and the effects that such incidents may have on the learner (Cross et al., 2016; Sezer, Yilmaz, & Yilmaz, 2015). Only if cyber-users are aware of cyber-risks and the implications thereof can cyber-users attempt to be cyber-safe. There was both a need and a desire for such cyber-safety awareness and training among the interviewed teachers. Some recommendations by the teachers included the following:

- Implement methods and monitor plans to support the cyber-safety initiatives in schools;
- Include cyber-safety in the school curriculum;
- Improve cyber-safety education for teachers; and principals through training and
- Assist schools in implementing cyber-safety procedures.

The current research revealed that teachers have a basic awareness of cyber-safety and are concerned about educating their learners, but they lack the necessary knowledge and skills to address this issue. Unless the above-mentioned countermeasures are urgently implemented in the South African school system, the cyber-safety situation will deteriorate. If teachers' and principals' knowledge and skills regarding cyber-safety are not improved, it will be to the detriment of school learners.

Table 3 presents a critical overview of current cyber-safety initiatives in South Africa. The table is structured to show the status of policies and procedures, training, material and distribution methods at the school level in South Africa.

Most of the aspects mentioned in Table 3 are long-term activities that will take time to plan, design and implement. Ultimately, a country should have a long-term commitment and initiatives to enhance awareness regarding cyber-safety (Labuschagne & Eloff, 2014). However, long-term

planning and implementation will not solve the direct cyber-threat to school learners over the next few years. According to the WolfPack report, South Africa should first focus on short-term initiatives and then move on to medium- and long-term initiatives (Wolfpack Information Risk, 2013). The planning of long- and short-term initiatives is depicted in Figure 2.

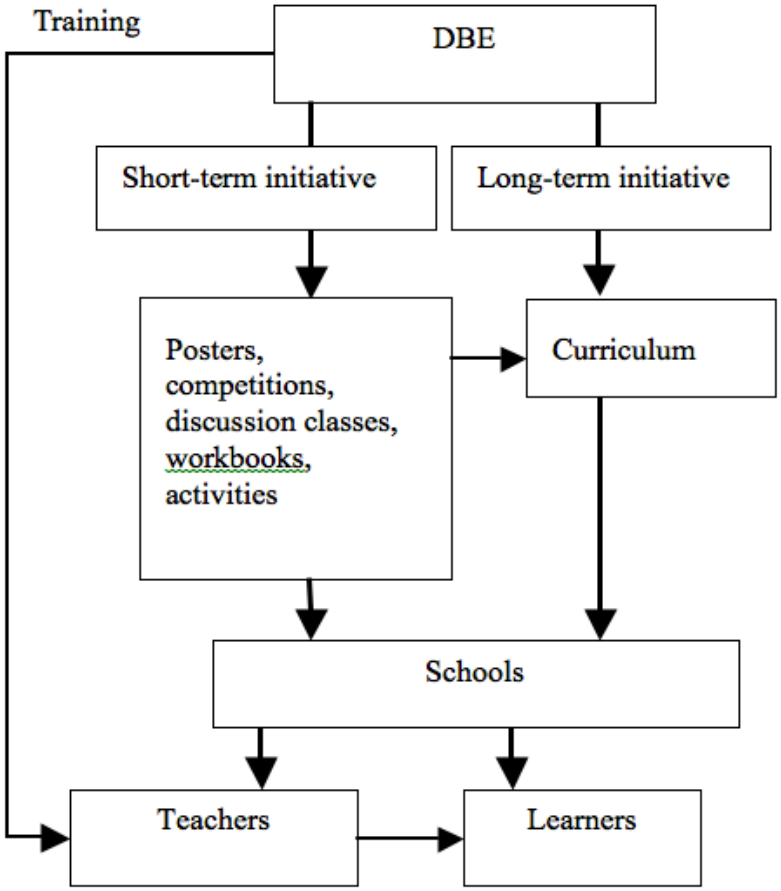

Figure 2: Long and short-term initiatives (adapted from (Kritzinger, 2014))

http://dx.doi.org/10.18489/sacj.v28i1.369

Table 3: Critical overview of cyber-safety awareness methods/process in South Africa

POLICIES AND PROCEDURES	
National cyber-safety curriculum	No curriculum through government Proposed curriculum through academia
National cyber-safety policy for school learners	1. National Cyber Security Policy Framework for South Africa 2. Child Protection Act 3. Cybercrimes and Cybersecurity Bill 4. Guidelines on e-Safety in Schools Note: the above legislation/bills/acts/guidelines provide fragmented sections (if any) on how to deal with cyber-safety among school learners within the school environment. Implementation of these documents has been very limited.
National cyber-safety incident handling system for cyber-safety incidents within the school environment	South Africa has implemented the CSIRT initiative but this is more focused on industry and does not focus on incidents within the school environment.
TRAINING	
Government and DBE Academia / Industry	Websites established Yes – at a cost to the trainee
MATERIAL	
Posters Games Printed workbooks	Yes – academia, government and industry Yes – academia and industry Yes – academia and industry
DISTRIBUTION METHODS	
Through government Through industry and academia	No (only web presence) To a degree (workshops)

http://dx.doi.org/10.18489/sacj.v28i1.369

The rest of this paper will focus on a short-term approach towards creating and implementing initiatives to promote awareness about cyber-safety in schools. The research points to the importance of long-term cyber-safety awareness initiatives, policies and legislation to establish a long-term culture of cyber-safety within the school environment. However, owing to the current lack of long-term initiatives in South Africa, the short-term option is a more immediate approach. Nevertheless, while short-term projects are used to improve the cyber-safety culture in the short term, long-term projects/policies must be readied and implemented as soon as possible, alongside training for teachers on cyber-safety and handling cyber-safety incidents within the school environment.

Various short-term cyber-safety initiatives can be implemented within a school environment. Examples of such initiatives include: posters, workbooks, workshops, competitions, discussion forums and classroom activities. The rest of the research and assessment of the short-term approach focused on the use of posters within the school environment. The poster that was used for testing the short-term approach was designed as a cyber-safety pledge as an inexpensive method of conveying the concept of cyber-safety. The "My cyber-safety pledge" poster was designed especially for this research and was based on the following 12 cyber-safety "rules":

1. I will avoid giving out any personal details such as my name, address, phone number, email, password or school name.
2. I will avoid opening emails, files or web pages from people I don't know or trust.
3. I will always check with an adult before downloading.
4. I will never respond to strangers online.
5. I will tell an adult if something or someone online makes me feel uncomfortable, scared or confused.
6. I will tell an adult if anyone online asks to meet me in person.
7. I will block unwanted communication.
8. I will remember that posted information cannot be deleted.
9. I will think before I post.
10. I will use privacy settings on social media sites.
11. I will avoid sending any pictures of myself to strangers.
12. I will ask permission before posting photos of other people.

The "My cyber-safety pledge" poster was used to test if short-term initiatives would have an impact on school learners' awareness of cyber-safety. The 12 points of the "My cyber-safety pledge" poster were adopted and adapted from the national "Safer Internet Day" promoted within the USA, EU and Australia on an annual basis (Insafe, 2016).

http://dx.doi.org/10.18489/sacj.v28i1.369

6 POST-STUDY AND DATA ANALYSIS

The pledge poster was distributed to 250 schools in South Africa through the Pick n Pay School Club project. The Pick n Pay schools project is a South African project that supports and distributes educational resources through private sector funding. This project aims to deliver, cultivate and contribute to the current educational system in South Africa. The Pick n Pay project was used as a result of its access to school teachers and school learners. A total of 8 750 teachers were reached and 187 500 learners participated in the pledge poster initiative across the following provinces of South Africa:

- Eastern Cape: 30 schools;
- KwaZulu-Natal: 40 schools;
- Northern Cape: 8 schools;
- Free State: 30 schools;
- Limpopo: 23 schools;
- North West: 18 schools;
- Gauteng: 50 schools;
- Mpumalanga: 10 schools; and
- Western Cape: 41 schools.

Teachers from each school were requested to rate the value of the "My cyber-safety pledge" poster. The rating method included a 5 point quality rating point scale; 'very poor', 'poor', 'average', 'good' and 'excellent' (Taylor-Powell, 2008).

In the feedback received, 33% of the educators indicated that the material was excellent and 67% rated it as good. No poor or average results were received.

In the feedback received regarding the increase in learners' awareness of cyber-bullying, 50% of the teachers indicated that their perception of an increase in cyber-safety awareness was excellent and 50% indicated that it was good. No poor or average results were received.

In respect of the educational value of the topics covered, 50% of the teachers rated it as excellent and 50% rated it as good. No poor or average results were received.

Teachers provided an average rating of 8,9 out of 10 for the quality of the material provided and an average rating of 9,1 out of 10 for the likelihood of using the content in their classroom. In respect of the usefulness of the content, 77% of the teachers rated it as excellent, 21% rated it as good and 2% rated it as average. No poor results were received.

Feedback from teachers at the participating schools regarding the "My cyber-safety pledge" poster was as follows:

http://dx.doi.org/10.18489/sacj.v28i1.369

- Teachers were very appreciative of the awareness that the pledge was creating regarding cyber-bullying;
- Teachers indicated that the pledge was excellent. The pledge received an overall rating of 5 out of 5;
- Teachers indicated that the poster would help students to become aware of the dangers of the internet;
- Teachers felt that cyber-bullying was a big issue in schools. Since technology was constantly changing and here to stay, they felt that more posters on this kind of topic were needed and
- Teachers appreciated the cyber-safety poster as it dealt with an important issue that affected many children on a daily basis.

An overall analysis of the results of the research project indicated that short-term initiatives (even small initiatives) did have an impact on cyber-safety awareness among teachers and school learners. The results of the research indicated that short-term cyber-safety initiatives were an option for cultivating a culture of cyber-safety awareness in schools. Such initiatives were even more important for lower LSM schools that did not necessarily have the funding to pay a third party to assist with cyber-safety policies and procedures. The findings proposed that future work should include conducting the post-study again with more initiatives, for example with workbooks, workshops and classroom activities, especially among lower LSM schools in South Africa.

7 CONCLUSION

Access to ICT devices and internet/cyber-connectivity is on the rise in South Africa, as in many other developing countries. Access to cyber-space is no longer a luxury, but an everyday activity for many teachers and learners in the school environment. This study investigated the situation regarding cyber-safety awareness in South African schools. The results from the pre-study indicated that there was a dire need for material and guidance to ensure that school learners would be aware of issues relating to cyber-safety.

The research found that almost 50% of the schools that participated in the survey did not have a cyber-safety policy in place. From the 50% of schools that did have policies, teachers indicated that they would prefer these policies to be standardised by the Department of Basic Education. The research also indicated that 88% of teachers in the study agreed that learners were exposed to cyber-risks. Two-thirds (66%) of the teachers indicated that they felt ill-equipped to respond to cyber-incidents within the school.

Altogether 92% of the teachers felt that cyber-safety should be included in the curriculum to equip the learners with a basic understanding of cyber-safety. The research proposed that a short-term approach be introduced to ensure that school learners have access to cyber-safety material to improve their cyber-safety awareness. A poster containing cyber-safety guidelines for school learners was

designed as part of the research. A post-study was conducted to establish if the proposed short-term cyber-safety initiative would assist school teachers in improving the cyber-safety knowledge of their learners. Virtually all the teachers reported that such an approach was assisting the learners and increased their cyber-safety awareness. It was agreed that the poster of the cyber-safety pledge could be used effectively as an inexpensive short-term initiative to start the process of establishing a national cyber-safety culture among school learners.

References

Badenhorst, C. (2011). Legal responses to cyber bullying and sexting in South Africa. Centre for Justice and Crime Prevention (CJCP) Issue Paper 10.

Byron, T. (2008). Safer children in a digital world: The report of the Byron Review. Department for Children, Schools and Families. Retrieved from http://dera.ioe.ac.uk/7332/7/Final%20Report%20Bookmarked_Redacted.pdf

CJCP & UNICEF. (2013, November). Connected dot com: Young people's navigation of online risks. Last accessed: 13 Jul 2016. Retrieved from http://www.unicef.org/southafrica/resources%5F14002.html

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., … Barnes, A. (2016). Longitudinal impact of the Cyber Friendly Schools program on adolescents' cyberbullying behavior. *Aggressive Behavior*, *42*(2), 166–180. http://dx.doi.org/10.1002/ab.21609

De Lange, M. (2012). *Guidelines to establish an e-Safety awareness in South Africa* (Master's thesis, Nelson Mandela Metropolitan University).

De Lange, M. & Von Solms, R. (2012). An e-Safety educational framework in South Africa. In *Southern Africa Telecoms and Network Applications Conference (SATNAC)*.

Della Cioppa, V., O'Neil, A., & Craig, W. (2015). Learning from traditional bullying interventions: A review of research on cyberbullying and best practice. *Aggression and Violent Behavior*, *23*, 61–68. http://dx.doi.org/10.1016/j.avb.2015.05.009

ENISA. (2010, November). The new users' guide: How to raise information security awareness. Last accessed: 13 Jul 2016. Retrieved from https://www.enisa.europa.eu/publications/archive/copy%5Fof%5Fnew-users-guide

Furnell, S. (2010). Jumping security hurdles. *Computer Fraud & Security*, *2010*(6), 10–14. http://dx.doi.org/10.1016/S1361-3723(10)70067-1

Govender, I. & Skea, B. (2015). Teachers' understanding of E-Safety: An exploratory case in KZN, South Africa. *Electronic Journal of Information Systems in Developing Countries*, *70*.

Grobler, M. & Dlamini, Z. (2012). Global cyber trends: A South African reality. IIMC International Information Management Corporation. IIMC International Information Management Corporation.

Hanewald, R. (2008). Confronting the pedagogical challenge of cyber safety. *Australian Journal for Teacher Education*, *33*(3), 1–16. http://dx.doi.org/10.14221/ajte.2008v33n3.1

Insafe. (2016). Safer Internet Day. Last accessed: 13 Jul 2016. Retrieved from https://www.saferinternetday.org/

ISC Africa. (2015). Local resources: Industry initiatives and public awareness. Last accessed: 13 Jul 2016. Retrieved from http://cybercrime.org.za/local-resources/#awareness-campaigns

Jobi, T. & Kritzinger, E. (2014). Online awareness among Sepedi school children in South Africa. In *Ireland International Conference on Education (IICE-2014)*.

Kortjan, N. & Von Solms, R. (2012). Fostering a cyber security culture: A case of South Africa. In *ZA-WWW, 2012 Conference*.

Kortjan, N. & Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*, *52*. http://dx.doi.org/10.18489/sacj.v52i0.201

Kortjan, N. & von Solms, R. (2012). Cyber security education in developing countries: A South African perspective. In *International conference on e-Infrastructure and e-Services for developing countries* (pp. 289–297). Springer.

Kouadio, Y. M. (2008, March). The digital divide still an issue. Retrieved from http://epub.uni-regensburg.de/10713/

Kouttis, S. (2016). Improving security knowledge, skills and safety. *Computer Fraud & Security*, *2016*(4), 12–14. http://dx.doi.org/10.1016/S1361-3723(16)30037-9

Kritzinger, E. (2014). Online safety in South Africa–a cause for growing concern. In *2014 Information Security for South Africa* (pp. 1–7). IEEE.

Kritzinger, E. & Padayachee, K. (2013). Engendering an e-safety awareness culture within the South African context. In *AFRICON, 2013* (pp. 1–5). IEEE. http://dx.doi.org/10.1109/afrcon.2013.6757708

Kruger, H. A., Drevin, L., Flowerday, S., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. In *2011 Information Security for South Africa* (pp. 1–7). IEEE.

Labuschagne, W. A. & Eloff, M. (2014). The effectiveness of online gaming as part of a security awareness program. In *13th European Conference on Cyber Warfare and Security (ECCWS-2014), the University of Piraeus, Piraeus, Greece* (p. 125).

Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G., & Ólafsson, K. (2014). Net children go mobile: The UK report. Net Children Go Mobile. Retrieved from http://eprints.lse.ac.uk/59098/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Livingstone,%20S_EU%20Kids%20Online_Livingstone_Net_%20children_%20go_2014_Livingstone_Net_%20children_%20go_2014_author.pdf

Miles, D. (2011). Youth protection: Digital citizenship–principles & new resources. In *2011 second worldwide cybersecurity summit (WCS)* (pp. 1–3). IEEE.

Mwim, E. & Kritzinger, E. (2014). Proposed countermeasures to reduce the cyber divide: A South African perspective. In *African Cyber Citizenship Conference 2014 (ACCC2014)* (p. 90).

Perren, S., Corcoran, L., Cowie, H., Dehue, F., Mc Guckin, C., Sevcikova, A., … Völlink, T., et al. (2012). Tackling cyberbullying: Review of empirical evidence regarding successful responses by students, parents, and schools. *International Journal of Conflict and Violence*, *6*(2), 283.

Porter, G., Hampshire, K., Abane, A., Munthali, A., Robson, E., Bango, A., … Milner, J. (2015). Intergenerational relations and the power of the cell phone: Perspectives on young people's

phone usage in sub-Saharan Africa. *Geoforum*, *64*, 37–46. http://dx.doi.org/10.1016/j.geoforum.2015.06.002

Sezer, B., Yilmaz, R., & Yilmaz, F. G. K. (2015). Cyber bullying and teachers' awareness. *Internet Research*, *25*(4), 674–687. http://dx.doi.org/10.1108/IntR-01-2014-0023

Smit, D. (2015). Cyberbullying in South African and American schools: A legal comparative study. *South African Journal of Education*, *35*(2), 01–11.

Symantec. (2013). 2013 Norton Report. Last accessed: 13 Jul 2016. Retrieved from https://www.symantec.com/about/news/resources/press%5Fkits/detail.jsp?pkid=norton-report-2013

Taylor-Powell, E. (2008). Wording for rating scales. Last accessed: 13 Jul 2016. Retrieved from http://www.uwex.edu/ces/4h/evaluation/documents/Wordingforratingscales.pdf

von Solms, S. & von Solms, R. (2014). Towards cyber safety education in primary schools in Africa. In *Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)* (pp. 185–197).

Wolfpack Information Risk. (2013). The 2012/2013 SA Cyber Threat Barometer Report. Last accessed: 13 Jul 2016. Retrieved from https://www.wolfpackrisk.com/south-african-cyber-threat-barometer/