SACJ 29(2) October 2017
Research Article

Growing a cyber-safety culture amongst school learners in South Africa through gaming

Elmarie Kritzinger

University of South Africa

ABSTRACT

Virtually all school learners today have access to ICT devices and the internet at home or at school. More and more schools are using ICT devices to improve education in South Africa. ICT devices and internet access have enormous advantages and assist learners in learning and teachers in teaching more successfully. However, with these advantages come numerous ICT and cyber-risks and threats that can harm learners, for example cyber-bullying, identity theft and access to inappropriate material. Currently, South Africa does not have a long-term plan to grow a cyber-safety culture in its schools. This research therefore proposes a short-term initiative in the form of a game-based approach, which will assist school learners in becoming more cyber safe and teach learners about the relevant cyber-related risks and threats. The research is based on a quantitative survey that was conducted among primary school learners to establish if the game-based approach would be a feasible short-term initiative. The aim of the research is to establish if a game based approach can be used to improve cyber-safety awareness. This approach was plotted into the required ICT and cyber-safety policy required by all schools.

Keywords: cyber-safety, school learners, game, awareness

Categories: • **Social and professional topics ~ Informal 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 (CORRESPONDING)

Article history:
Received: 01 Mar 2017
Accepted: 23 Aug 2017
Available online: 13 Oct 2017

1 INTRODUCTION

Information and communication technology (ICT) has become an integral part of modern society, as well as a necessity in all aspects of our lives. It is used in all areas – from education, socialising and information gathering to being the foundation of industrial processes. ICT has enormous benefits provided that it is used correctly (Byron, 2008; Cross et al., 2016). If technology is used incorrectly, it can lead a number of cyber-related risks and threats which include access to inappropriate material (pornography), personal information being compromised (identity theft), and emotion-related

Kritzinger, E. (2017). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal 29*(2), 16–35. https://doi.org/10.18489/sacj.v29i2.471

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

threats (cyber-bullying) (Atkinson, Furnell, & Phippen, 2009; S. von Solms & von Solms, 2014; Chandrashekhar, Muktha, & Anjana, 2016; Sezer, Yilmaz, Yilmaz, & Gizem, 2015; Huda et al., 2017). These cyber-risks can have physical and psychological effects on the users, especially school learners (Watts, Wagner, Velasquez, & Behrens, 2017).

A growing number of school learners are exposed to technology at an early stage of their life (Chandrashekhar et al., 2016; Srivastava, 2017; Rigby, 2017). The age of learning about and experimenting with technology, cyber space and social media starts as early as primary school. Learners consider technology to benefit their social interaction with friends and as important in finding information.

In Kritzinger (2014), the following statistics regarding school learners and their cyber activities (in South Africa) were reported:

- 82% of learners have access to the internet from inside their bedrooms.
- 35% of learners hide their online activities from their parents.
- 15% of learners use their cell phones during school hours, even if this is against school rules.
- 61% of parents and teachers do not monitor learners' internet use.
- In the case of 62% of learners, no parental guidance software is installed to regulate the children's internet access.
- 63% of learners access inappropriate internet material.
- 93% of learners believe that there are possible dangers and threats associated with internet use.

These statistics indicate that school learners with access to ICT devices connect to the internet (cyber space) and become vulnerable to cyber-risks and threats. School learners are spending more time online than ever before (Park, Na, & Kim, 2014). It is therefore essential that school learners be educated about protecting themselves (and their information) in the cyber environment (Cross et al., 2016; Kritzinger, 2014). It is the responsibility of all role players (parents, guardians, teachers and government) to ensure that all school learners who have access to ICT protect themselves and their information (de Lange & von Solms, 2012; Department of Basic Education, RSA, 2015). Although role players will never be able to ensure 100% cyber-safety (Byron, 2008), an effort must be made to minimise risk as school learners have become a "soft" target for cyber crime.

It is vital to involve all role players in ICT and cyber-safety awareness, especially schools that provide or have access to ICT devices in the school environment. ICT use in schools is becoming the norm and an increasing number of learners are exposed to ICT devices at school, ranging from cell phones, tablets to computer labs (Department of Basic Education, RSA, 2012; de Lange, 2012). Currently, many parents and teachers do not have the capacity or self-confidence to address cyber risk, with the result that problems such as cyber-bullying are a major concern (Cross et al., 2016; de Lange & von Solms, 2012).

cyber-safety is a critical issue in various (developing) countries in Africa (Kortjan & von Solms, 2014), but this paper focuses on the situation in South Africa. South Africa is a developing country where urgent intervention is needed to ensure that school learners are cyber safe (Kritzinger, 2014; Grobler & Dlamini, 2012; R. von Solms & van Niekerk, 2013). Various strategies have been introduced to improve ICT and cyber-safety, such as workshops, posters, workbooks, brochures, discussion classes and gaming (Ibrahim & Jaafar, 2009; Abawajy, 2014).

The research that is reported on in this article focused primarily on improving cyber-safety awareness and proposed a game-based approach among primary school learners in South Africa. The aim of the research is to prove the feasibility of a gaming as a method that can be used by schools and parents to establish (grow) a cyber-safe ICT culture.

In Section 2 of this paper, cyber-safety and the challenges facing some developing countries in creating and implementing initiatives to improve the current situation are discussed. Section 3 addresses the gaming based approach while Section 4 describes the methodology used within this research. Section 5 discuss the findings of the survey conducted as part of the research, namely whether a game-based approach could be used as a short-term initiative to improve ICT and cyber-safety awareness. Section 6 provides some overview of the cyber-safety culture that must be in place at schools to ensure cyber-safety by suggesting a fundamental approach to what is needed by schools to create and implement an ICT and cyber-safety policy (or subpolicy). Section 7 concludes this research.

2 CYBER-SAFETY

The normalisation of the internet has been accompanied by a set of more critical discourses concerning the potential abuse of technology, particularly because of some users' propensity for non-conformist, unethical or deviant behaviour while online (Selwyn, 2008). The internet has paved the way for many new forms of irregular behaviour (Freestone & Mitchell, 2004), such as dishonest, disruptive or deviant online activities and actions.

These irregular behaviours can be classified under cyber crime and cyber misbehaviour (Selwyn, 2008). School learners are at risk if they do not understand the dangers of their own cyber activities (S. von Solms & von Solms, 2014). Cyber-risks can range from identity theft and cyber-bullying to sexting, all of which have social implications for the school learner. It is therefore essential that all school learners with access to ICT educated on how to identify and minimise possible cyber-risks and to be cyber safe.

2.1 Cyber-safety awareness around the world

The pedagogy for educating school learners about cyber-risks should be the same as in the traditional education of learners on ethics and the principle of "doing no harm". Although the cyber environment is based on real life, it must be seen as an extension of real life and not as a separate entity. All ethical principles that are implemented in real life must therefore be transferred to the cyber world, which is a bit tricky, since the cyber world is often anonymous with few or no rules to govern cyber space. It is nevertheless vital to educate all school learners properly on cyber-safety, cyber ethics and the use of ICT.

A number of developed countries have already included cyber-safety in their school curricula. The government of the United Kingdom (UK) decided to educate school learners aged 11 to 14 on cyber security (Farrell, 2014). Australia also put a number of cyber-safety measures in place to protect their learners (Department of Communications and the Arts, Australia, 2014). Other developed countries that are actively involved in teaching cyber-safety awareness are the United States of America, New Zealand and Canada (Kortjan & von Solms, 2014).

This is unfortunately not yet the case in numerous developing countries, especially in Africa. Africa is regarded as a collection of developing countries with a lack of knowledge of and skills in cyber-safety (Dlamini, Taute, & Radebe, 2011). Since fast-growing access to the internet makes African countries vulnerable to cyber attacks (Grobler & Dlamini, 2012), some countries have started the process of dealing with cyber-safety among learners, for example Tunisia (Cole et al., 2008), Rwanda and Mauritius (Dlamini et al., 2011). However, the majority of African countries – among them South Africa, Uganda, Sudan, Egypt, Morocco and Kenya – do not yet have measures in place to ensure proper cyber-safety among their school learners (S. von Solms & von Solms, 2014).

Africa has a high level of computer illiteracy and ineffective legislation (Grobler & Dlamini, 2012), which has resulted in South Africa being third highest on the list of countries with a high rate of cyber crime (Symantec Corporation, 2013). The rest of this paper will therefore focus on South Africa and its cyber-safety position, especially among school learners.

2.2 Cyber-safety in South Africa

A limited number of government initiatives have been launched to improve cyber-safety for South African school learners (Kortjan & von Solms, 2014). In addition, no cyber-related topics are included in the local school curriculum (Kritzinger & Padayachee, 2013). This lack of information about cyber-safety practices in the curriculum is largely due to insufficient action on the part of the South African government. The absence of cyber awareness as a life skill in the school curriculum has opened the door for school learners to become cyber victims.

An aggravating aspect is the general lack of knowledge and skills of South African teachers in respect of cyber-safety. Teachers are not properly trained in ICT and therefore not knowledgeable about cyber-safety. They have limited ICT knowledge and skills, and are ill-equipped to assist the learners (S. von Solms & von Solms, 2014) or handle ICT and cyber-related incidents.

Further barriers that have a direct impact on cyber-safety in South Africa include language, access to technical infrastructure and geographical location. Language as a barrier to learning is more extensive if countries have multiple official languages, such as South Africa, which has 11 official languages. South African legislation makes provision for all school learners in the Foundation Phase (up to Grade 3) to be educated in their home language. Jobi and Kritzinger (2014) investigated whether cyber-safety awareness was influenced by language. The study was conducted among 100 Sepedi-speaking school learners and 30 teachers at a Sepedi school. The results indicated that the majority of school learners would prefer to receive tuition about cyber-safety in their home language (e.g. Respondent 1: "I would be happy if we are taught about online risk in a class as a lesson in Sepedi").

It is therefore important that all the relevant official languages be taken into consideration when cyber-safety measures are put in place. This is of value not only to the school learners, but also to the teachers.

2.3 Current status

From the discussion thus far (Kritzinger, 2015), it is evident that the current situation in South Africa regarding cyber-safety awareness for school learners is as follows:

- There is neither commitment from the South Africa government to enhance cyber-safety awareness among school learners, nor are there any policies that protect learners if cyber incidents occur.
- There is no commitment to implement cyber-safety education in the school curriculum.
- Teachers and schools are ill-equipped to implement cyber-safety initiatives by themselves – they have a lack of knowledge about ICT, and are also hampered by severe time and financial constraints.
- Schools are not yet properly equipped with the necessary infrastructure to resolve problems with ICT devices and access.
- The different economic, language and educational barriers in South African schools contribute to the lack of a cyber-safety culture in South Africa.
- Limited cyber-related initiatives are being implemented by the South African government.

Given the absence of cyber-safety awareness in the school curriculum, as well as the language barriers in South Africa, gaming is proposed as a possible intervention to enhance cyber-safety among school learners.

Gaming was identified as a method of education that can be used online or be physically presented to raise cyber-safety awareness among learners. Games can be translated into any language and distributed to urban and rural schools at minimal or no cost and so engage both school learners and teachers in the cyber environment. Gaming can effectively be used as a short-term approach to improve ICT and cyber-safety awareness, while allowing government the necessary time to implement a more sustainable long-term approach (i.e. inclusion in the curriculum) (Kritzinger, 2016).

3 CYBER-SAFETY GAMES

Educational research has shown that school learners prefer games as learning tools (Ibrahim & Jaafar, 2009; Reid & van Niekerk, 2014). Computer games should engage learners with appropriate activities to ensure that learning takes place (Fisch, 2005). These games have been used mostly in developed nations to convey information about cyber-safety. Countries with established technology support, infrastructure and an integrated curriculum are generally more open to online games, whereas schools in developing countries face numerous challenges regarding an inadequate technology infrastructure and school curriculum, as well as language barriers.

An integrated school curriculum should therefore be adapted in developing countries to focus on online and offline games, while also ensuring that school learners are well aware of cyber-risks.

According to Fisch (2005), educational computer games can be played offline by using skills and concepts implemented in real life. It is also important to note which skills and knowledge obtained through offline games can be transferred to the online environment. The research on which this article is based supports both online and offline games to enhance cyber-safety among school learners. It investigated gaming as a possible tool to educate cyber-users (school learners and teachers) in respect of cyber-risks, including countermeasures:

- cyber-bullying
- sexting
- identify fraud
- phishing scams
- protecting personal information safe – privacy
- passwords
- posting on social media platforms
- online etiquette
- posting of multimedia (photos)

These are only a few examples of cyber-related issues that school learners must be aware of. It is also important to note that different risks and threats are appropriate for different age groups.

The research focuses on both online and offline games in this article which includes two offline games and one online game for school learners between 7 and 13 years old and therefore cyber-risks such as sexting have not been included in this research due to the age of the learners.

4 METHODOLOGY

The research was based on a positivist paradigm and the researcher adopted a deductive approach. The quantitative strategy was applied and a survey was used in this research. The survey was ethically approved for data collection among primary school learners. All educational and parental consent was obtained prior to the data-gathering phase. The first phase of the research included the design of games with a main focus on improving cyber-safety awareness. The second phase of the research focused on testing the games to investigate if gaming could be used to improve cyber-safety awareness among school learners.

The project adopted a quantitative approach to researching the impact of cyber-safety awareness games on primary school learners. Altogether 47 questionnaires were completed but one questionnaire had to be disregarded due to incomplete data. The results are therefore presented based on 46 completed questionnaires. All participating parents filled in the ethical consent forms and completed the questionnaires on behalf of both the learners and themselves. Ethical clearance was also obtained for this study.

5 QUALITATIVE STUDY ON CYBER-SAFETY AWARENESS GAMES

Three honours level students participated in this research project. Each honours student was requested to design a cyber-safety game that could stimulate the awareness of school learners regarding protecting themselves online. The students had to adhere to the following specifications (Kritzinger, 2015):

- School learners should be able to play the game online or have physical access to it.
- The game should be created as an online application printed in hard copy format.
- It must be translated into different languages.
- It must be cost effective to produce.
- It must be freely available to all school learners.
- It must be easy to distribute to all schools.
- It must enhance cyber-safety awareness (must have an educational factor).
- It must provide different levels of cyber-safety awareness.
- It must have a simple format (in terms of playing pieces, for example, board, dice and place holders).
- The game must have a South African flavour (where applicable).
- It must provide supporting material if needed (for different role players).
- It must support different learning styles.
- It must support different learning stages.

All three games displayed a minimum of 75% adherence to the pre-set requirements mentioned above. Two of the games were board games and could be easily distributed to school learners. The third game (an online game) could only be distributed to schools that had a computer lab or used by learners who had access to the internet at home.

All three games were found to provide knowledge and learning opportunity to a target group aged between 7 and 13 years (primary school). Each game was tested with a different group of participants.

The three game developers were to specify the design method, which included the following eight game-based factors:

1. Approach: The presentation material of the game
2. Players: Number of players in the game
3. Knowledge: The process through which the player obtained knowledge
4. Target driven: Reason to play the game
5. Opportunity: The opportunity for each player to win the game.
6. Level to advance: Can the player(s) advance to a next level of play?
7. Educational game: Are opportunities provided to improve the player's knowledge about the given topic?
8. Age appropriates: Can the game be adopted to target a specific age group?

Table 1 depicts the design factors for each of the games.

	Game 1	Game 2	Game 3
1	Board game	Board game	Online game
2	Multiple players	Multiple players	Single player
3	Question and answer	Question and answer plus actions	Actions plus events
4	Competitive	Goal-driven	Task-driven
5	Equal	Random	Player-specific
6	No	No	Yes
7	Yes	Yes	Yes
8	Yes	Yes	Yes

Table 1: Game-based design factors

Each game was evaluated on a 4-point Likert scale ranging from poor, average, good to very good. The pre-set condition was that the designed games had to obtain 75% of a combined score of "good" and "very good". All three game prototypes complied with this condition and were therefore approved for this research and to be part of the qualitative survey approach.

All the games were tested by means of the same pre-set questionnaire that consisted of the following sections:

- Section A: Biographical information (five questions)
- Section B: Child's cell phone/internet use (four questions)
- Section C: Cyber-safety awareness (six questions)
- Section D: Cyber-safety awareness game (four questions)

Section A obtained information regarding the age of the learner, school environment, gender and access to technology (cell phones and the internet).

Section B determined whether the learners asked permission to use the devices, whether the learners' activities were monitored by the parents and whether the parents discussed cyber-risks with the learners.

Section C included questions on the cyber-safety awareness of the learners and the parents/teacher, as well as whether such a topic should be incorporated into the school curriculum. The section concluded by asking details regarding possible cyber-risks to which learners might be exposed.

The last section (section D) concluded the survey by testing out the cyber-safety awareness game. Questions included whether the game was easy, whether it improved the learners' cyber-safety awareness and whether the language of the game was appropriate.

Section 5.1 deals with the data that was obtained from the research process (questionnaire). The questions were asked to primary school learners whose age ranges are depicted in Figure 1.

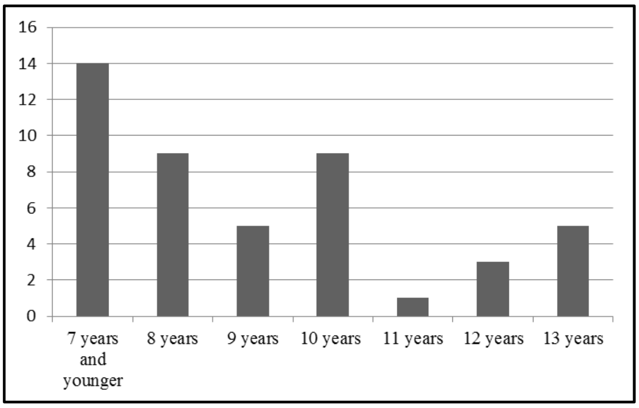

Figure 1: Ages of the participants

The gender of the learners was 41% female and 59% male. Sections B-D of the questionnaire are reported on in Sections 5.1 to 5.4.

Age	Participants	Access	No Access
13	5	5	0
12	3	3	0
11	1	1	0
10	9	9	0
9	5	5	0
8	9	4	5
Under 7	14	8	6

Table 2: Access to cell phones

	Yes (%)	No (%)	Not specified (%)
Send and make calls	52	37	11
Send/receive SMS	50	37	13
Play games	87	9	4
Use social networks	24	59	17
Surf the internet	46	39	15
Use MXit/Facebook	13	67	20
Visit chat rooms	11	70	20
Take pictures	78	15	7
Other purposes	17	33	41

Table 3: Actions performed on cell phones

5.1 Mobile use

This section of the questionnaire was used to investigate access to cell phones among primary school learners. Only 28% did not have access to a cell phone (only among learners 8 years or younger). All learners in the age group 9-13 years had cell phones as indicated in Table 2.

Of the learners who had cell phones, 72% had access to the internet. Their online activities related to internet use are depicted in Table 3.

Table 3 shows that 87% of the school learners' actions (time) were spent on game play. It is on the basis of this finding that the researcher proposed that ICT and cyber-safety can be improved through gaming.

5.2 Permission and monitoring

This section of the questionnaire dealt with the involvement of parents and teachers in online access of the learners. The results indicated that 33% of the learners did not ask permission to use cell phones and the internet from either their parents (at home) or teachers (at school). The researcher used two questions (age and permission) to establish that a third of the learners who did not ask permission were in fact 9 years or older. The group up to 8 years old still asked permission to use technology.

The parents and teachers were asked if they monitored the activities of the learners; the results indicated that cell phone and internet activities of 34% of the learners were not monitored. No correlation could be found between age, permission and monitoring of activities by parents and teachers. This section also explored the basic cyber-safety knowledge of the learners and parents. Parents indicated the level of the cyber-safety awareness of their children as depicted in Figure 2.

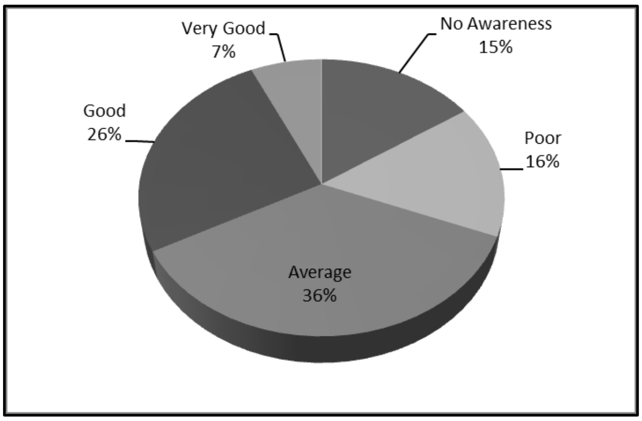

Figure 2: Cyber-safety awareness status of the learners

When the categories “very good” and “good” were combined, they reflected the perceived awareness status of 33% of learners. The “average” category accounted for 36% of learners and the categories “no awareness” and “poor” accounted for a combined 31%. This indicates that there was some degree of cyber awareness among the school learners. The parents were requested to indicate their own cyber awareness on the same scale and these findings are depicted in Figure 3.

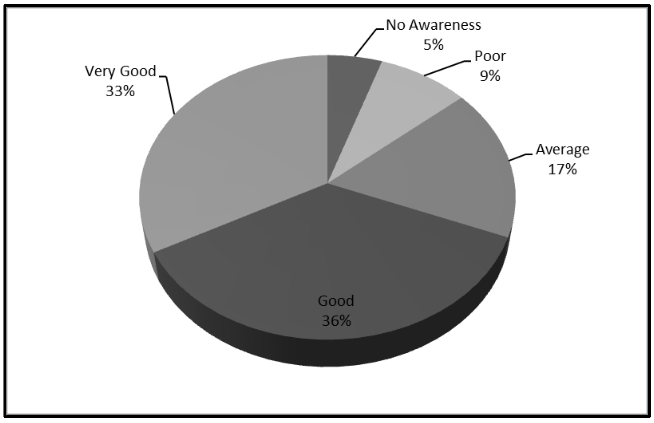

Figure 3: Cyber-safety awareness of the parents

https://doi.org/10.18489/sacj.v29i2.471

When Figure 2 and Figure 3 are compared, it indicates that only 36% of the learners had cyber awareness equal to that of the parents. Altogether 64% of the learners had a lower awareness level than the parents.

Sixty-one per cent of the learners who had access to technology stated that their parents patiently discussed cyber-safety risks with them. The remainder (39%) did not discuss cyber risk with their children, who were 9 years or younger. No correlation was found between age of the learners, access to technology, permission required and discussion of cyber-risks. This indicates that cyber-safety awareness must still be established and developed among school learners. The next section focuses on the different online and cyber-risks that can occur when school learners are cyber active.

5.3 Potential cyber-risks

The research investigated the different risks that can affect a learner's cyber environment. Table 4 depicts the percentage of participants who had been exposed to the cyber-risks listed.

	Responses (%)
Identity theft	57
Invitations to pornography	74
Pornography sites	74
Thieves obtain residential address	59
Airtime thieves	54
e-Money withdrawals	37
cyber-bullying	78
Other	24

Table 4: Cyber-safety risks

The results in Table 4 clearly indicate that even when basic cyber-safety awareness is in place, school learners are still exposed to cyber-risks. As much as 78% of the children had been exposed to cyber-bullying, which is a major public health problem that is directly linked to serious mental, social and academic consequences for school learners (Cross et al., 2016).

Almost three out of four learners (74%) had been exposed to pornography and pornography sites. It is therefore vital that school learners are equipped with awareness on the ethical use of ICT devices and the internet. The current research proposes that this awareness should be incorporated into the school system to ensure that all learners become aware of their own cyber-safety.

5.4 Language used in cyber materials

Mwim and Kritzinger (2016) found that language is not a factor that has a direct impact on digital device and internet use among adults. The research reported on in this paper subsequently investigated if this was the same for learners. All the games designed for the current research were designed and tested in English. The findings indicated that language does play a role in the education of learners, especially those aged 7-13.

Of the 42 respondents, almost half indicated that they would have preferred the game in another language. This is in line with the finding by Kruger, Flowerday, Drevin, and Steyn (2011), who indicated that primary school learners must be educated in their mother tongue. Seeing that South Africa has 11 different official languages, this factor must be taken into consideration. When games or any other cyber-awareness safety materials are used/designed for primary school learners, the language medium must be a factor in designing the game. Designed games must be easy to translate into different languages.

5.5 Cyber-safety awareness improved by gaming

The questionnaire asked if the parents felt that cyber-safety awareness should be part of the national school curriculum, and all (100%) of the parents supported this notion. This is a very important finding to highlight, since cyber-safety awareness is currently not included in the South African school curriculum at all.

The participants were asked if gaming improved the cyber-safety awareness of school learners and the results are depicted in Figure 4.

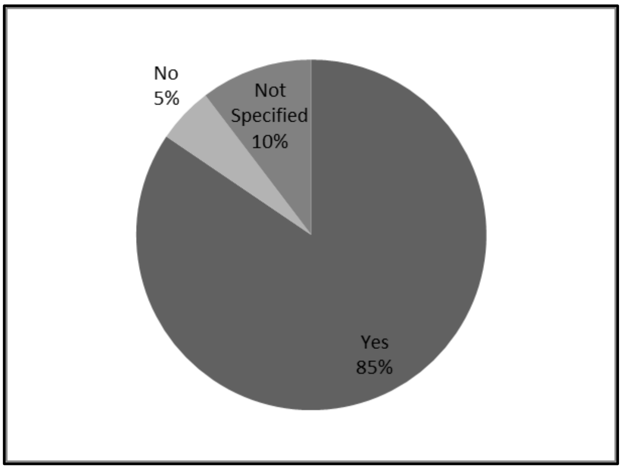

Figure 4: Improved cyber-safety awareness

The results in Figure 4 indicate that gaming can be used as a successful medium to improve cyber-safety awareness among school learners. Altogether 85% of the participants supported the game approach to this end. However, it is important to note that gaming in itself is not the only and complete solution for learners' insufficient cyber-safety awareness. It may nonetheless offer a remedy over the short term.

98% of all the participants indicated that they would prefer ICT and cyber-safety to be a formal part of the South African school curriculum. However, a proper long-term approach that includes

ICT and cyber-safety education in the school curriculum will not be realised within the next few years. Until this is a reality, it is vital to use short-term initiatives such as gaming to ensure that all school learners are made aware of ICT and cyber-safety issues and learn how to protect themselves on or outside the school grounds.

The environment that should be created in schools to ensure that initiatives such as gaming are effective is discussed below.

6 AN ICT AND CYBER-SAFETY POLICY FOR SCHOOLS

The current research focused on investigating whether gaming can be used to improve cyber-safety awareness among school learners, parents and teachers. It identified specific criteria for creating games, as well as topics on cyber and ICT issues that learners must be made aware of. However, the research found that gaming only constitutes a part of improving cyber-safety awareness and it must be combined with other educational methods to ensure a holistic ICT and cyber-safe environment at school (Department of Basic Education, RSA, 2015). It is vital for all schools to establish and implement appropriate ICT and cyber-safety policies.

6.1 The school's responsibility

Schools must have an ICT and cyber-safety policy in place that they make available to all parents and explain to all school learners.

Currently, the South African education system does not have a standard national ICT and cyber-safety policy to be implemented in all schools. It is therefore up to each school to create and implement a policy that is unique to that specific school. In terms of South African law, schools are ultimately responsible for the safety (physical and emotional) and wellbeing of learners on the school grounds. Schools (i.e. governing bodies) have a legal obligation to ensure cyber-safety awareness of all learners on the school grounds (de Lange & von Solms, 2012), especially when schools provide access to or expect learners to have and use ICT devices during school hours. If the school has no ICT and cyber-safety policy, it can be held accountable when a cyber incident takes place that compromises the physical or emotional wellbeing of a school learner. Even worse, a school cannot act against any possible cyber attack (e.g. cyber-bullying) if it does not have a proper policy in place.

It is vital that schools adopt a holistic approach and have a proper ICT and cyber policy (or even subpolicy) in place.

6.2 An ICT and cyber-safety policy

All schools must have a policy or subpolicy in place that directly addresses ICT and cyber-safety within the school. This policy (or subpolicy) must be linked to the South African School's Code of Conduct (Department of Basic Education, RSA, 2012; Sonhera, Kritzinger, & Loock, 2015). Some fundamental elements are proposed that should be included in a formal ICT and cyber-safety policy–something that is not provided by the Department of Basic Education.

An ICT and cyber-safety policy (or subpolicy) can be seen as a statement that is binding on the school, learners, parents and teachers. Seven elements that should be included in any such policy or subpolicy are discussed in the next section, namely general background and definitions; a committee for ICT and cyber-safety; teachers; school learners; parents; external role players, and a cyber-safety culture. Some other essential issues to be included in such a policy are discussed in the rest of this section.

6.2.1 Cyber-safety documentation

This section focuses on the content of what must be included in cyber-related documentation. It is important that all definition, actions and approaches is clearly defined and communicated to all participants. Some examples that must be included in cyber-related documentation.

- Definition of the extent of ICT and cyber use among teachers and learners on school grounds.
- Definitions of all ICT and cyber-related activities.
- Definition of ICT and cyber incidents.
- What is seen as misuse of ICT devices and negative cyber actions?
- How will the school respond to ICT and cyber-related incidents?
- Penalties imposed for violating the policy.
- Instrument(s) for monitoring ICT and cyber-related incidents.
- Feedback system to parents regarding incidents that have occurred.

Note that there is no "one size fits all" approach. Each school will have a different cyber-safety policy that is created for their environment and cyber needs.

6.2.2 Committee for cyber-safety

This section is about the committee that must be established at each school. The committee will consist of different role players that will have an impost on the cyber-safety policy.

- Must consist of teachers, parents and representatives of the governing body of the school.
- Must include an advisory representative
  - with a legal background;
  - with a counselling background;
  - from the Department of Education;
  - from the local SAPS.

- Must create an age-appropriate ICT and cyber-safety policy.
- Must ensure the implementation and monitoring of the policy based on issues – depending on the age appropriateness.
- Must ensure that all evidence of reported cyber incidents is correctly and accurately documented.

6.2.3 Teachers

It is vital that the school (committee) ensures that the teachers are also included in the cyber-safety awareness process. Some aspects that must be included in the cyber-safety policy include:

- All teachers must have the required cyber skills, knowledge and awareness.
- Teachers should be identified to act as contact points for learners to report cyber incidents.
- Teachers must provide physical and emotional counselling to school learners in the event of an ICT or cyber incident.
- Teachers should provide an effective reporting structure when an incident occurs.

6.2.4 School learners

It is vital that the school (committee) ensures that the learners are also included in the cyber-safety awareness process. Some aspects that must be included in the cyber-safety policy include:

- All learners must be made aware of the policy and of their role and responsibilities/rights to ensure a cyber-safe environment.
- All learners must be made aware of the penalties imposed for violating the policy.

6.2.5 Parents

It is vital that the school (committee) ensures that the parents are also included in the cyber-safety awareness process. Some aspects that must be included in the cyber-safety policy include:

- All parents must be made aware of the policy and of their role and responsibilities/rights to ensure a cyber-safe environment.
- All parents must be made aware of the penalties imposed for violating the policy.
- All parents must sign that they were informed of the school's cyber-safety policy.

6.2.6 External role players

It is vital that all external role players are identified to ensure correct measures are taken if a cyber-safety incident occurs. The cyber-safety policy must:

- identify external role players (for example SAPS and social workers);
- determine when external role players will be contacted and involved;
- define the process of involving external role players.

6.2.7 ICT and cyber-safety culture

It is vital that each school grow a cyber-safety culture to assist learners to be cyber safe as well as support learners that are cyber victims. The cyber-safety policy must include:

- all actions to be taken to improve the ICT and cyber-safety culture;
- awareness methods and tools that are age appropriate for the learner;
- the timeline and implementation of identified methods and tools.
- Different cyber-related topics that will be used for cyber-safety awareness.

6.3 Discussion of an effective cyber-safety policy

The final drafted policy will differ from school to school due to the differences in levels of ICT devices, use of the devices and access to the internet. However, most policies will address the same basic and problematic cyber-related risks, for example cyber-bullying, which usually occurs via cell phones between learners from the same school. Stating the required levels of teacher training, education and awareness is an essential element of a school's cyber-safety policy. Schools must ensure that teachers have the proper skills, knowledge and expertise to identify cyber-risks and handle cyber incidents when they occur.

All role players must be made well aware of the policy and its contents; each participant must know his/her role, responsibilities and rights, as well as the penalties if the policy is violated.

Issues related to ICT and cyber-safety should no longer be seen as luxuries that are isolated to and affect only a few advantaged schools. Cell phone and internet use have become so widespread that cyber-safety challenges have become commonplace in all schools and among all school learners. Schools in South Africa therefore have the responsibility to ensure that their learners obtain the necessary ICT and cyber-safety awareness and that the necessary support is made available to protect each and every school learner. The school must identify different appropriate and feasible cyber-safety methods and measures to increase the cyber-safety culture within a school. This research proposed gaming as one possible option for schools to improve cyber-safety awareness amongst school learners. The proposed game approach address the language issue of educating within South Africa as games (online and board games) can be easily and at limited cost be translated in different languages.

7 CONCLUSION

This research study investigated whether gaming is a feasible short-term initiative to address cyber-safety challenges in South African schools. The study identified a number of key issues that are currently lacking in relation to cyber-safety awareness and education in South Africa. These key issues include access to ICT, language barriers and an overall lack of educational material dealing with cyber-safety. Schools have the responsibility to ensure that school learners are ICT and cyber safe on the school grounds. The growing use of ICT devices and the increase in cyber-related activities taking place in schools require from schools to take note of and ensure that plans are in place to guarantee a safe ICT and cyber environment. This study suggests that gaming can be used by teachers and parents to improve learners' ICT and cyber-safety, and it provides certain fundamental guidelines regarding the basic elements of an ICT and cyber-safety policy that must be created and implemented in every school in South Africa.

The current research also indicates that game-based learning can be successfully used to promote cyber-safety awareness among school learners. Future research will include repeating this study to determine the extent to which active learning takes place when learners play cyber-safety awareness games. Such future research will also focus on whether gaming can assist learners to convert cyber-safety knowledge into appropriate cyber-safety behaviour or actions.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: Enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13–19. https://doi.org/10.1016/S1361-3723(09)70088-0

Byron, T. (2008). Safer children in a digital world: The report of the Byron Review: Be safe, be aware, have fun. Last checked: 27 Sep 2017. Department for Children, Schools and Families. Retrieved from http://dera.ioe.ac.uk/7332/7/Final%20Report%20Bookmarked%5FRedacted.pdf

Chandrashekhar, A., Muktha, G., & Anjana, D. (2016). Cyberstalking and cyberbullying: Effects and prevention measures. *Imperial Journal of Interdisciplinary Research*, *2*(3), 95–102.

Cole, K., Chetty, M., LaRosa, C., Rietta, F., Schmitt, D. K., Goodman, S. E., & Atlanta, G. (2008). *Cybersecurity in Africa: An assessment*. Atlanta, Georgia, Sam Nunn School of International Affairs, Georgia Institute of Technology.

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. https://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 *Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*.

Department of Basic Education, RSA. (2012). Guidelines on e-Safety in schools: Educating towards responsible, accountable and ethical use of ICT in education. Last checked: 27 Sep 2017. Retrieved from http://goo.gl/mxK0xa

Department of Basic Education, RSA. (2015). The national school safety framework. Last checked: 03 Oct 2017. Retrieved from https://goo.gl/zpxmj8

Department of Communications and the Arts, Australia. (2014). Enhancing online safety for children bill 2014. Last checked: 02 Oct 2017. Retrieved from https://goo.gl/rmfpqU

Dlamini, I., Taute, B., & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. In *Proceedings of South African Cyber Security Awareness Workshop (SACSAW)* (pp. 15–31).

Farrell, N. (2014). Government to give kids cyber security lessons. Last checked: 27 Sep 2017. Retrieved from http://www.techradar.com/news/software/security-software/government-to-give-kids-cyber-security-lessons-1233480?src=rss&attr=al

Fisch, S. M. (2005). Making educational computer games educational. In *Proceedings of the 2005 conference on Interaction design and children* (pp. 56–61). ACM. https://doi.org/10.1145/1109540.1109548

Freestone, O. & Mitchell, V. (2004). Generation Y attitudes towards e-ethics and internet-related misbehaviours. *Journal of Business Ethics*, *54*(2), 121–128. https://doi.org/10.1007/s10551-004-1571-0

Grobler, M. & Dlamini, Z. (2012). Global cyber trends a South African reality. In *IST-Africa 2012 Conference Proceedings* (pp. 1–8). IIMC International Information Management Corporation.

Huda, M., Jasmi, K. A., Hehsan, A., Mustari, M. I., Shahrill, M., Basiron, B., & Gassama, S. K. (2017). Empowering children with adaptive technology skills: Careful engagement in the digital information age. *International Electronic Journal of Elementary Education*, *9*(3).

Ibrahim, R. & Jaafar, A. (2009). Educational games (EG) design framework: Combination of game design, pedagogy and content modeling. In *Electrical Engineering and Informatics, 2009. ICEEI'09. International Conference on* (Vol. 1, pp. 293–298). IEEE. https://doi.org/10.1109/ICEEI.2009.5254771

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

Kortjan, N. & von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), 29–41. https://doi.org/10.18489/sacj.v52i0.201

Kritzinger, E. (2014). Online safety–awareness vs. implementation: A South African study. In *Proceedings of the 43rd Annual South African Computer Lecturers Association 2014*.

Kritzinger, E. (2015). Enhancing cyber safety awareness among school children in South Africa through gaming. In *Science and Information Conference (SAI), 2015* (pp. 1243–1248). IEEE. https://doi.org/10.1109/SAI.2015.7237303

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

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

Kruger, H. A., Flowerday, S., Drevin, L., & Steyn, T. (2011). An assessment of the role of cultural factors in information security awareness. In *Information Security South Africa (ISSA), 2011* (pp. 1–7). IEEE. https://doi.org/10.1109/ISSA.2011.6027505

Park, S., Na, E.-Y., & Kim, E.-m. (2014). The relationship between online activities, netiquette and cyberbullying. *Children and youth services review*, *42*, 74–81. https://doi.org/10.1016/j.childyouth.2014.04.002

Reid, R. & van Niekerk, J. (2014). Snakes and ladders for digital natives: Information security education for the youth. *Information Management & Computer Security*, *22*(2), 179–190. https://doi.org/10.1108/IMCS-09-2013-0063

Rigby, K. (2017). School perspectives on bullying and preventative strategies: An exploratory study. *Australian Journal of Education*, *61*(1), 24–39. https://doi.org/10.1177/0004944116685622

Selwyn, N. (2008). A safe haven for misbehaving? An investigation of online misbehavior among university students. *Social Science Computer Review*, *26*(4), 446–465. https://doi.org/10.1177/0894439307313515

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

Sonhera, N., Kritzinger, E., & Loock, M. (2015). Cyber threat incident handling procedure for South African schools. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance (HAISA) 2015* (pp. 215–232).

Srivastava, J. S. (2017). Cyber crime: Kids as soft targets. *International Journal of Innovative Computer Science and Engineering*, *4*(1), 31–36.

Symantec Corporation. (2013). Norton report 2013. Last checked: 27 Sep 2017. Retrieved from https://www.symantec.com/about/newsroom/press-kits/norton-report-2013

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

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

Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature review. *Computers in Human Behavior*, *69*, 268–274. https://doi.org/10.1016/j.chb.2016.12.038