A Cyber Safety Model for Schools in Mozambique

Martina J. Zucule de Barros and Horst Lazarek
Institute of Systems Architecture, Technical University of Dresden, Helmholtzstr. 10, 01069 Dresden, Germany

Keywords: Cyber Risks, Cyber Safety, Awareness, Model, Mozambique.

Abstract: The use of the internet and Information Technology (IT) provide innumerable facilities for individuals. Children and young people are the most active group who use and explore all the facilities promoting their social well-being. However, all of these facilities also pose several risks especially for children and young people. Online dangers such as cyberbullying, child pornography and identify theft represent a danger for them. Thus, educate them about online dangers is a crucial aspect. Worldwide, especially in developed countries many initiatives have been implementing to raise awareness and educate children and young people how to behave safely in cyberspace. In developing countries for instance, in African countries these type of initiatives are at its infancy stages or does not exist. Currently, there is lack of these initiatives in Mozambique. Therefore, this paper proposes a cyber safety model for primary and secondary schools in Mozambique to address this gap and promote a cyber safety culture among children and young people.

1 INTRODUCTION

Cyberspace and the use of technological devices is increasingly transforming the life of children and young people. European Union (EU) Kids Online stated that "young children from zero to eight years have show special increased patterns of internet use" (Holloway et al., 2013). On the other hand, tweens between nine and twelve years internet usage mirrors the teenagers (five to six) years and the younger school children internet usage increased to the same level of previous tweens usage (Holloway et al., 2013). Moreover, the EU Kids Online also stated that "the rapidity with children and young people are gaining access to online, convergent, mobile and networked media is unprecedented in the history of technological innovation" (Livingstone et al., 2012). However, this is not a new phenomenon. Since 1990, the use of electronic media by children and youth has been growing systematically (Tomczyk and Kopecky, 2016). Indeed the use of internet provides many facilities especially for children and young people such as worldwide cross-cultural interactions, academic support, development of interpersonal and critical thinking, social support and identity exploration (Mishna et al., 2009). However, all of these facilities can cause many risks to them because "the online environment is a very dangerous area for which young people are not equipped" (Kritzinger, 2016). Moreover, policy resources for protection are usual directed to older children where most of the concern is concentrated on teenagers (Holloway et al., 2013).

In 2016, a study conducted by the European Computer Driving Licence (ECDL) stated that the most vulnerable groups online is composed by children and young people. Despite the extensive illusion that young people are digital natives and can use digital technologies safely and efficiently, they are not outside of cyber risks (ECDL, 2016). The EU Kids Online report (Livingstone et al., 2012) argued that the risks related to children internet use is classified in terms of content, contact and conduct. The content is related to child as receiver of mass produced message (e.g. violent or gory content, pornographic content, racist hateful and embedded marketing). The contact is related to child as participant in adult initiated online activity such as harassment, stalking, grooming sexual abuse or exploitation, ideological persuasion and personal data misuse. Conduct is related to child as actor, perpetrator or victim in peer-to-peer exchange covering bullying, hostile peer activity, sexual harassment, potentially harmful user generated content and gambling copyright (Livingstone et al., 2015).

In developed countries several cyber safety initiatives targeting groups such as children, young people, teachers and parents have been implementing. For instance, in USA computer-security and internet safety training programs were created in school curriculum for K-12 level (Zepf, 2013). They were created be-

Barros, M. and Lazarek, H.
A Cyber Safety Model for Schools in Mozambique.
DOI: 10.5220/0006573802510258
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 251-258
ISBN: 978-989-758-282-0

cause "it has been seen that foreign language acquisition has been especially effective at early stages in child development. Thus, it has been argued that young people should learn secure IT use and cyber safety early in their careers" (Zepf, 2013). Therefore, it is important that young people are being exposed to cyber security principles that will protect them and their environment from danger experiences. Thus, this paper proposes a cyber safety model for primary and secondary schools in Mozambique aimed at raising awareness, education and promote a cyber security culture.

2 ANALYSIS OF CHILDREN CYBER SAFETY INITIATIVES

2.1 Developed Countries

In developed countries several initiatives such as cyber safety awareness campaigns, games and introduction of cyber safety topics in school curriculum have been implementing to keep children and young people safe online. In USA, despite the existence of cyber safety programs in elementary schools other programs have been developing by the government and also public/private sectors. The National Cyber Security Alliance (NCSA) is a public/private partnership responsible for the *staysafeonline* project www.staysafeonline.org/ and the C-SAVE, a volunteer program focused on young people to teach them cyber security, cyber safety and cyberethics. Moreover, students have the possibility to use support materials to help them on their online experiences (NCSA, 2017). In 2009, the Department of Homeland Security (DHS) developed the "Stop.Think.Connect" initiative (Zepf, 2013). It was developed to promote cyber security awareness in USA targeting several groups including children and young people.

In European Union (EU) , the European Strategy for a Better Internet for Children has been a central reference document regarding children cyber safety since its publication in 2012. The strategy has four main pillars (1) stimulating quality content online for young people, (2) stepping up awareness and empowerment, (3) creating a safe environment for children online and (4) fighting against child sexual abuse and exploitation. It addresses several actions to be undertaken by the European Commission (EC), member states and whole industry value chain. Furthermore, online safety was included as a specific topic in the school curriculum of 23 education systems across Europe (EC, 2012). Moreover, the EU also launched the Happy Onlife (HOL) game and toolkit "to build and develop safety and knowledge on internet use, overuse and abuse" (EU, 2016). The game aims to raise awareness about the risks and opportunities of the internet and promote best online practices. It targets children, parents and teachers. The toolkit also contains "a project booklet with a collection of educational activities promoting shared experiences of the digital world among teachers, parents and children between eight and twelve years" (EU, 2016).

In 2010, the United Kingdom (UK) Council for Child Internet Safety (UKCCIS) was established. It is a group composed by more than 200 organizations from government, law, academic, industry and charity sectors working in partnership to help keep children safe online (Gov.UK, 2017). The UKCCIS education group has conducted severals activities such as production of a guidance for schools governors to help governing boards support their school leaders to keep children safe online, advices for schools and colleges related to online incidents and creation of guide for parents related to safer use of social media (Gov.UK, 2017). Moreover, Internet Service Providers (ISPs) in UK have adopted the code of practice on parental control that promotes active choice where customers are asked at the moment of purchase whether they want to have parental controls and offer them free of charge (EC, 2012). In Estonia, almost all the daily life activities rely on internet. Thus, the Estonian Safer Internet Centre is responsible for promoting safer and better use of internet and mobile technologies among children and young people. It is also responsible for conducting activities such as organize seminars and training sessions for children, parents, teachers and social workers, compile and publish training and awareness raising materials for them and disseminate informative and educational material nationally and internationally (ESIC, 2017).

In Germany, klicksafe (EU, 2017) is an awareness campaign that promotes media literacy and adequate handling of the internet and new media. The goal is to make public more conscious of the importance of safe internet use for children and adolescents. The project targets parents, educators, teachers, social service and youth workers. It also provides education material for teachers and online seminars for multipliers as well as information material for parents. Several stakeholders such as Deutsche Telekom and some governmental sectors such as die Bundesregierung, Bundespruefstelle fuer jungendgefaehrdende Medien and Bundesamt fuer Sicherheit in der Informationstechnik (BSI) sponsor the initiative (EU, 2017). Moreover, a certified youth protection software can be used to prevent

children from accessing websites providing harmful content. In other EU countries this type of provision does not exist, but countries such as UK, Spain, Italy and Czech Republic implement other reporting mechanisms for harmful and illegal content and behavior supported by several stakeholders such as NGOs, police and industry (EC, 2012).

In Australia, the government recognizes "that students safety and well-being are essential for academic and social development. Students should be able to learn and develop in safe, supportive and respectful environments" (Gov.AU, 2016). Therefore, Australian schools, families and communities have the accountability to provide safe online environment and teach children how they should use technology in positive and fruitful ways. The Department of Education works with the Department of Communications which has the responsibility for cyber safety matters along with the Australian Communications and Media Authority to ensure cyber safety education to all Australian schools. The following initiatives providing information for students, parents and community were developed (Gov.AU, 2016):

- Student Wellbeing Hub (www.studentwellbeinghub.edu.au/): It is an online platform to assist Australian schools and communities to nurture student responsibility and resilience to build a positive schools culture.
- Bullying No Way (www.bullyingnoway.gov.au/): It is an educational website for school communities and general public. The website also provide online curriculum and other resources to support bullying prevention.
- The Office of the Children e-Safety Commissioner (www.esafety.gov.au/): It is an online safety platform with a vast amount of actualized information and resources, coupled with comprehensive complaints scheme to assist children and young people who experience serious cyberbullying.

2.2 Developing Countries (Africa Countries)

On the contrary to developed countries, developing countries especially African countries face several challenges to develop and implement cyber safety initiatives because, African countries are characterized by limited knowledge, expertise and understanding of cyber safety. Furthermore, schools do not have curricula or extramural for cyber safety education and young children are at risks as they may not know the dangers associated with the cyberspace (von Solms and von Solms, 2014). Moreover, many African countries "have higher level of computer illiteracy and ineffective legislation" (Kritzinger, 2015). Despite that some countries, have been making noticeable efforts for instance, Tunisia, Rwanda and Mauritius have started programs to deal with cyber safety among children (Kritzinger, 2015). On the other hand, Uganda and South Africa have developed initiatives to raise cyber awareness for young people. In Uganda, the Internet Society (ISOC) Uganda Chapter developed the online Safety Education Kit for young people between five and twenty years to stimulate and prevent online victimization by teaching them how to stay safer online and offline. The kit contains the following resources (IS, 2014):

- Online safety resources: Contains online safety guides.
- Online safety pledges: Guides for safer internet use for primary and secondary schools.
- Online safety rules and posters: Poster with online safety rules.

In South Africa, the South African Cyber Security Academic Alliance (SACSAA) (www.cyberaware.org.za/) was established in June 2011. The main goal of the SACSAA "is to campaign for the effective delivery of cyber security awareness throughout South Africa to all populations groups" (UNISA, 2017). This initiative is being conducted by research groups from University of Johannesburg (UJ), Nelson Mandela Metropolitan University (NMMU) and University of South Africa (UNISA). In addition, a cyber security awareness project was developed to assist cyber users with limited understanding and knowledge regarding cyber security to protect themselves and their information. It targets children, adults and eldery. The UNISA *My Cyber Safety Pledge* is one of the cyber safety school project. It is a poster dedicated to educate learners about cyber bullying containing rules on how to safer behave on cyberspace and encourage them to take the cyber safey pledge (UNISA, 2017).

2.3 Findings

From the analysis of the initiatives in developed countries one can notice that several stakeholders are working together to raise cyber safety, but the role played by the government is crucial for instance, in countries such as Australia, USA, UK and Germany its noticeable the governments actions. In EU, countries such as UK and Germany have additional mechanisms for children online safety (e.g. code of practice on parental control (UK) and the certified youth

protection software in Germany). On one hand, these additional measures can have national positive impacts, but on the other hand, it shows that not all children in EU have the same online protection. Despite that a common aspect in many developed countries, is that the majority of the initiatives also target teachers, parents and social workers. The approach adopted by developed countries is emphasized on the Guidelines for Policy Makers on Child Online Protection published by International Telecommunication Union (ITU) which states that national level government agencies, ISPs, teachers, parents organizations, public and private sectors, children and young people are relevant stakeholders in children cyber safety (ITU, 2009). In developing countries especially African countries, despite the existence of some cyber safety initiatives the lack of the government leadership is noticeable.

3 CHILDREN CYBER SAFETY INITIATIVES IN MOZAMBIQUE

In 2013, the Ministry of Education and Human Development (MEHD) published the strategic education plan regarding Information and Communication Technologies (ICTs). It does not mention any initiative related to cyber safety for schools (MEHD, 2013). Moreover, the content of ICTs lectures does not include cyber safety. This means that there is a lack of information related to cyber safety practices in the school curriculum and currently, there is no led by the government on this regard. Therefore, school children have a higher risk to experience cyber attacks due to the lack of cyber security awareness. Nonetheless, the strategic education plan (2012-2016) states that "despite the acknowledge of ICT in improving the quality of education and institutional development, the integration of ICT in the curriculum as means of teaching and communications is still limited. The major challenges contributing to this are related to" (MEHD, 2013):

- Availability of suitable infrastructure.
- Lack of skills in IT maintenance.
- Insufficient funds to maintain the computer laboratories in operation.

Despite that the strategic education plan, also mention the following outlined activities to strengthen ICTs in Mozambican schools considering three key elements (MEHD, 2013):

- Teachers with the responsibility to promote ICTs as an instrument for the teaching-learning process.
- Schools who stimulates the use of ICTs to create an efficient, effective and transparent administrative and management system.
- Classroom. It is important the use of ICTs in classrooms as a learning tool to improve the quality of education.

Therefore, the problem of ICTs in schools has three factors teachers do not dominate very well ICTs, Mozambican schools do not have a robust ICT infrastructure and there is a general lack of knowledge and skills regarding cyber safety. However, a major challenge for the MEHD is that the use of ICTs in Mozambican schools did not achieved the desired levels. Teachers do not dominate ICTs tools, because they are poorly trained, consequently this influences the learning process because the students will also lack the basic knowledge and skills to use ICTs to contribute to their learning process and social well-being. On the other hand, there is a lack of training for teachers regarding cyber safety. This means that currently, teachers are not capable to assist students. Nevertheless, the language is also an important aspect in developing countries. Kritzinger (Kritzinger, 2015) stated that "a number of developing countries have language as en educational barrier". Mozambique has Portuguese as the official language, but the country also has another local languages.

3.1 Discussion

In the previous section, the current situation related to cyber safety initiatives in Mozambican schools were addressed. From these analysis it is evident the lack of cyber safety awareness and education for children and young people. Therefore, the following aspects were addressed:

- The general lack of leadership by the Mozambican government to raise cyber safety awareness among schools.
- The lack of policies that protect young people if cyber incidents take place.
- Teachers lack dominance of ICTs tools.
- Schools have problems to properly manage their ICTs infrastructure.
- The Mozambican government has not implemented any cyber related initiatives.

Due to the current situation, this paper proposes a cyber safety model for schools in Mozambique has a solution to change the current situation.

3.2 Approaches to Develop a Cyber Safety Awareness Programme

In USA, the National Institute of Standards and Technology (NIST) published the Building an Information Technology Security Awareness and Training Program. It states that three major steps such as designing the program, developing the awareness and training material and implementing the program are important steps in the development of an IT security awareness and training program. Moreover, it also presents the following three common approaches/models to design, develop or implement an awareness and training program (NIST, 2003):

- Model 1: Centralized Program Management Model where a central authority is responsible for coordinating the entire IT security awareness and training program.
- Model 2: Partially Decentralized Program Management Model. In this model, the central authority defines the security awareness and training policy and strategy, but the implementation is delegated to other units.
- Model 3: Fully Decentralized Program Management Model. In this model, the central authority is responsible for disseminating broad policy and expectations regarding security awareness and training requirements, but other organizational units have responsibility for executing the entire program.

In all three models, the communication between the central authority and other units travels in both directions. In EU, the European Network and Information Security Agency (ENISA) published the The new users guide: How to raise information security awareness (ENISA, 2010). The guide aims to provide a practical and effective advice to public and private organizations seeking to prepare and implement information security awareness initiatives. The ENISA guide states that the development of an information security awareness programme consist of three main processes plan, asses and design, execute and manage and evaluate and adjust (ENISA, 2010).

4 PROPOSAL OF A CYBER SAFETY MODEL

The European Strategy for a Better Internet for Children states that "schools are digital and media literacy and skills are crucial to children's use of the internet. As children start using the internet at very young age, it is necessary for online safety education to start in early childhood... and schools are best placed for reaching the majority of children, regardless of age, income or background, as well as other key recipients of internet safety messages, such as teachers and (indirectly) parents" (EC, 2012). Therefore, the proposed model focuses primary and secondary schools and is based on NIST model 2 and the ENISA guide. Both approaches were chosen considering the country context. On the other hand, from the analysis of developed as well as developing countries, it is noticeable the existence of an entity responsible for carrying out children cyber safety initiatives. This model is not a complete solution, but it represents the starting point as a form to enhance the current situation in Mozambique. The model namely, e-Safety aims to raise and promote cyber safety culture. Therefore, Mozambican schools need a model to assist them in providing:

- Awareness for children and young people about the risks and dangers in cyberspace and countermeasures.
- Training for school teachers and parents about cyber security, its risks and measures to avoid them.

This model also aims to change the behavior of the users regarding the use of the internet and technological devices and provides children's internet literacy. The DHS stated that some issues that kids face online include, cyber predators, cyberbullying and identity theft. Therefore, this model will also focus on these topics (DHS, 2009). The following are the core elements of the e-Safety model:

- Government.
- The role players.
- International Cooperation.
- Identification of cyber safety topics.
- Supporting materials.
- Delivery

Figure 1 illustrates the cyber safety model with the respective elements. In the remaining parts of this section each element is discussed in more detail.

4.1 Government

The government is the key element of this model and represent the central authority. Kouttis stated that "government and schools must do its part to foster large scale awareness regarding cyber security and integrate it into the core curriculum as soon as students are using computing devices" (Kouttis, 2016). The Report on risks faced by children online and policies

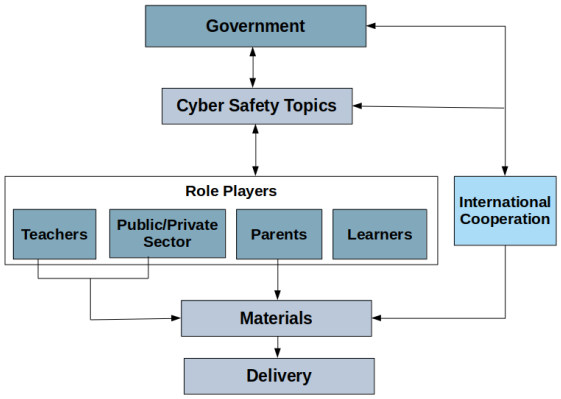

Figure 1: e-Safety Model for Primary and Secondary Schools

to protect them published by Organization for Economic Co-operation and Development (OECD) recommends that governments should demonstrate leadership and commitment to protect children online by adopting clear policy objectives at the highest level of government, identify government bodies with responsibility and authority to implement these policies and developing policies that are inclusive of all stakeholders and rely on a mix of public and private voluntary and legal, awareness raising, educational and technical measures to protect children online (OECD, 2012).

4.2 Role Players

The role players include the following elements:

- Teachers: Teachers play a key role in ensuring children safer online behavior. Teachers are required to tackle both the instructional side and the personal and social educational side of cyber safety (Simandl and Vanicek, 2017). They are expected to set good examples to young people related to the use of IT (Simandl and Vanicek, 2017). However without special preparation they will not have better knowledge and skills regarding cyber safety.
- Parents: Parents represent an important element in this process because as main caregivers they take care of their children and teach them how they should behave in society (Shin and Kang, 2016). They should control their children online activities and behavior contributing to help them to develop safer responsibilities. Moreover, EU Kids Online argued that education material for parents should consider the children age groups (Holloway et al., 2013).
- Learners: In this case learners covers kids, teens and youth. The ITU Guidelines for Children on Child Online Protection (COP) states that "there is no silver bullet solution to protect children and young people online. It requires a response from all society segments, including children and young people themselves" (ITU, 2016). Therefore, the model also considers learners as an important role players. It is important consider the difference among these three groups regarding the content of cyber safety. EU Kids Online (Holloway et al., 2013) recommends that internet safety education should focus all children age groups including pre-primary school or nursery/kindergarten and the content should be age-appropriate.
- Public and Private sector: The government has the responsibility to engage stakeholders and facilitate coordination of efforts. Countries such as UK and Australia have created new bodies to coordinate the activities of public and private sectors (OECD, 2012). For instance, the UK Council for Child Internet Safety an the Australian Consultive Working Group on cyber safety. The OECD Report states that the key role played by private sector actors to protect children online is broadly recognized (OECD, 2012). Therefore, this model also cover public and private sector as an important role player.

4.3 International Cooperation

Several international initiatives on children online protection exist. For instance, the ITU's COP Initiative and the EU Kids Online project (OECD, 2012). In 2012, the Global Alliance Against Child Abuse Online (www.europa.eu/rapid/press-release_MEMO-12-944_en.htm) was launched by the EC and USA aimed to raise standards worldwide and unite efforts around the world to effectively combat online sexual crimes against children. Currently, it is represented by 54 worldwide countries, all the EU members, USA and Australia but, Mozambique is not a country member. However, the OECD Report recommends governments to "strength international networks of national organizations dedicated to protect children online, share national policy approaches and support regional and international capacity building efforts to improve policy and operational measures to protect children on the internet, including sharing of education and awareness raising tools" (OECD, 2012).

4.4 Cyber Safety Topics

Topics are an important element to conducted cyber safety initiatives. Therefore, schools have the responsibility to verify which topics are essential and link them to a distinct role players. The following are some of them (Livingstone et al., 2015):

- Internet surfing
- Social networking
- Cyberbullying
- Child pornography
- Sexual images or messages
- Cyber identify theft
- Online privacy

However, it is also essential incorporate countermeasures to teach school how they can keep themselves safe online.

4.5 Support Materials

Support material is also important for all role players because they can enhance their skills and knowledge in relation to cyber safety. Therefore, materials such as posters, leaflets, books, newspaper articles, workshops and videos should cover cyber safety topics and they should be updated.

4.6 Model Phases

The model phases covers the delivery process. Countries such as USA, Australia, UK and Germany and Estonia have introduced cyber safety training for educators, parents and social workers. In addition, they also publish awareness materials to support them. Training educators and parents is also emphasized by OECD Report which recommends training educators and encourage other stakeholder to educate and raise awareness of children and parents (OECD, 2012). The following activities were identified:

1. Teachers training: Teachers should have sufficient skills and knowledge regarding cyber safety. Therefore, the government has the responsibility to provide training and assistance for them. The government can work with public/private sector or develop international cooperation to provide the adequate training for teachers.
2. Parents assistance: This phase can be lead by schools with the government help to define a program to assist parents regarding cyber safety.
3. Learners assistance: This phase is related to parents and learners. After acquiring the basic knowledge related to cyber safety parents should assist their children (e.g. teaching them how to safely use IT devices and behave safer in cyberspace).

5 CONCLUSIONS

The use of IT devices and internet provide several opportunities and benefits for children and young people. However, all of these opportunities also expose them to innumerable online dangers. Internationally several countries have been developing initiatives to keep children and young people safe online. Thus, this paper proposes an e-Safety Model for primary and secondary schools in Mozambique. The proposed model was based on the analysis of cyber safety initiatives from developed and developing countries as well as the NIST model 2 and ENISA guide. It is a response to the current lack of these initiatives in Mozambique and considers the country context. The model is composed by six elements such as government, role players, international cooperation, cyber safety topics, materials and delivery, where the government represents the key element. The e-Safey model aims to raise, promote cyber safey awareness, develop skills, knowledge and assist the young generation to promote and cultivate a cyber security culture. However, it is an abstract model. Therefore, a future work will be implement the e-Safety model and evaluate it. According to the results we will see if it helped to improve the current situation faced by Mozambican schools. Thereafter, it can be adjusted and re-launched.

REFERENCES

DHS (2009). Stop.think.connect national cybersecurity awareness campaign kids presentation. Available at https://www.dhs.gov/. Accessed: 2017/09/19.

EC (2012). Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions european strategy for a better internet for children. COM (2012) 196 final.

ECDL (2016). It security skills, protecting your children, your private life and your business. http://ecdl.org/policy-publications/it-security-skills. Accessed:2017/08/23.

ENISA (2010). The new users guide: How to raise information security awareness.

ESIC (2017). Targalt internetis. http://www.targaltinternetis.ee/. Accessed: 2017/08/23.

EU (2016). Happy onlife. https://web.jrc.ec.europa.eu/ happyonlife/. Accessed: 2017/08/09.

EU (2017). Klicksafe.de. http://www.klicksafe.de/. Accessed: 2017/08/16.

Gov.AU (2016). Cybersafety in schools. https://www.education.gov.au/cybersafety-schools. Accessed: 2017/08/16.

Gov.UK (2017). Uk council for child internet safety (ukccis). https://www.gov.uk/. Accessed: 2017/08/27.

Holloway, D., Green, L., and Livingstone, S. (2013). Zero to eight, young children and their internet use. Available at http://eprints.lse.ac.uk/ 52630/. Accessed on 24/08/2017.

IS (2014). Online safety education toolkit for young people in uganda. Available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front. Accessed: 2017/08/23.

ITU (2009). Guidelines for policy makers on child online protection.

ITU (2016). Guidelines for children on child online protection.

Kouttis, S. (2016). Improving security knowledge, skills and safety. In *Computer Fraud & Security*, volume 2016, pages 12–14. ScienceDirect.

Kritzinger, E. (2015). Enhancing cyber safety awareness among school children in south africa through gaming. In *Science and Information Conference (SAI*. IEEE.

Kritzinger, E. (2016). Cyber-safety a south african school perspective. Available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front.

Livingstone, S., Haddon, L., Goerzig, A., and Olafsson, K. (2012). Risks and safety on the internet, the perspective of european children. Available at http://eprints.lse.ac.uk/33731/. Accessed: 2017/08/18.

Livingstone, S., Mascheroni, G., and Staksrud, E. (2015). Developing a framework for researching childrens online risks and opportunities in europe. Available at http://eprints.lse.ac.uk/64470/.

MEHD (2013). Education strategic plan 2012-2016. http://www.mined.gov.mz/PROGS/Pages/plano-estrategico-educacao.aspx. Accessed: 2017/08/25.

Mishna, F., Saini, M., and Solomon, S. (2009). Ongoing and online: Children and youths perceptions of cyber bullying. In *Children and Youth Services Review*, pages 1222–1228. ScienceDirect.

NCSA (2017). C-save. https://staysafeonline.org/teach-online-safety/csave. Accessed: 2017/08/25.

NIST (2003). Building an information technology security awareness training program.

OECD (2012). The protection of children online recommendation of the oecd council, report on risks faced by children online and policies to protect them.

Shin, W. and Kang, H. (2016). Adolescents privacy concerns and information disclosure online: The role of parents and the internet. In *Computers in Human Behavior*, pages 114–123. ScienceDirect.

Simandl, V. and Vanicek, J. (2017). Influence on ict teachers knowledge and routines in a technical e-safety context. In *Telematics and Informatics*. ScienceDirect. In press, correct prof.

Tomczyk, L. and Kopecky, K. (2016). Children and youth safety on the internet: Experiences from czech republic and poland. In *Telematics and Informatics*, volume 33, pages 822–833. ScienceDirect.

UNISA (2017). Be aware, be cybersafe. http://eagle.unisa.ac.za/elmarie/index.php. Accessed: 2017/08/16.

von Solms, S. and 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)*. CSIR.

Zepf, A. L. I. (2013). Cyber-security curricula for basic users. Available at http://www.hsdl.org/?abstract&did=756406. Accessed: 2017/08/19.