Proceedings of the Eleventh International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2017)

Digital Wellness: Concepts of Cybersecurity Presented Visually for Children

S. von Solms[1] and R. Fischer[2]

[1] Department of Electrical Engineering, Faculty of Engineering and the Built Environment, University of Johannesburg
[2] African Centre of Excellence for Information Ethics, Department of Information Science, University of Pretoria
e-mail: svonsolms@uj.ac.za; rachel.fischer@up.ac.za

Abstract

From the minute that they are born, today's children are exposed to cyber space. These children grow up in a world where games are played online, plans are made over social media, friends communicate via chat groups and Google is the source of information for school projects. The digital world offers countless advantages for adults and children alike, but staying digitally safe should not only apply to adults paying their bills and doing online shopping. It is of critical importance to create awareness amongst children and young adults who are growing up using cell phones, tablets and computers. Unfortunately, education and awareness strategies and materials relating to cyber safety in South Africa are limited, which leads to children becoming increasingly more vulnerable to cyber-safety attacks. This paper presents the development of a children's book, entitled "Digital Well-nests: Let us play in safe nests" which was designed to assist in the digital wellness of young children. This book provides a visual representation of key concerns relating to cyber safety aimed at children.

Keywords

Awareness, Books, Children, Cyber Safety, Digital Wellness, Education

1. Introduction

The African digital landscape is unique as most of the technological advancement across the continent and South Africa (SA) has taken place in the mobile sphere. Unicef stated that "children and young people are leading the digital uptake in developing countries, but this also means that they are more likely to be exposed to negative online experiences". This calls true for SA as nearly 72% of mobile ownership was reported to be amongst 15 to 24-year olds in 2007 (South African Broadcasting Corporation and The Henry J. Kaiser Family Foundation, 2007) and that 58% of SA Facebook users fall within this age range (We are Social and Hootsuite, 2017).

Digital wellness refers to the notion of "being well in a digital society". is characterised by the ability of users to discern between the dangers and opportunities found in the cyberspace, act responsibly, and align their online behaviour with their offline values - to remain cyber safe. Currently there exist no formalised school curriculum to teach children to stay cyber safe in SA. As a result, SA has seen the

development of multiple online cyber safety education websites and learning material by universities, research institutions, private and public organisations in the attempt to keep kids safe (Google, 2017; South African Cyber Security Academic Alliance, 2015; Unisa, 2017; University of Pretoria, 2017). Many of these initiatives are digital or online initiatives where children complete online activities or watch online videos. However, not all children have dedicated access to the internet at school or at home to engage in all these activities, limiting the audience of digital cyber safety awareness campaigns. (Global Kids Online, 2016; Kritzinger, 2016). Research also shows that in the initial awareness-raising phase, campaigns must involve more than a website presence to create awareness and knowledge (CJCP and UNICEF, 2013; Kritzinger, 2016). In order to address this, a free cyber safety book was developed for young children to introduce children to the serious subject of cyber safety. This paper discusses the development of a children's rhyme book, entitled "Digital Well-nests: Let us play in safe nests", to assist in keeping South African children digitally safe.

The outline of the paper is as follows: Section 2 provides an overview of the South African digital landscape, where section 3 discusses cybersecurity education in SA. Section 4 provides a short overview on the contribution made by this work, while the book is discussed in detail in section 5. Section 6 concludes this paper.

2. South African Digital Landscape

TeleGeography forecasted in 2013 that Africa's demand for Internet access will grow by an average of 51% per annum (TeleGeography, 2013). In the first quarter of 2017, Africa had 985 million mobile subscriptions, with 9 million new subscriptions documented in the first quarter of 2017 (Ericsson, 2016). SA has the third highest number of mobile subscribers in Africa, with nearly 79.91 million subscriptions for a population of 55.21 million, (Unicef, 2012; We are Social and Hootsuite, 2017) equating to an estimated 72.9 % mobile ownership in 2007 where 78% of South Africans use the Internet via their mobile phones (Unicef, 2012; We are Social and Hootsuite, 2017).

The availability of the Internet to South African youth opens up many doors for education, learning and creativity. However, Unicef South Africa argues that children and young people, who are leading the digital uptake in developing countries, such as SA, are more likely to be exposed to negative online experiences (Unicef, 2016). The 2016 KidsOnline survey confirm this concern, as it was found that a large group of children have been exposed to hate speech (34.5%), gory images (32.7%), images of a sexual nature (51.2%) or sexual messages (Global Kids Online, 2016). The 2013 UNISA Cyber Security Awareness and Education Report stated that 93% of respondents believed that there exist possible threats online, where 65% stated that they are aware of cyberbullying incidents at their schools (Kritzinger, 2015). In reality, the integration of online devices in our society makes it near impossible to totally screen today's children from the dangers associated with the internet and social media. It is argued that children banned from using the internet and social media is more at risk, as they lack the skills to navigate safely

when they so find their way online and then may be unaware of how to seek help when trouble arises (Zeeko, 2017). It has been shown that technology can aid in safeguarding children, but that it alone cannot keep children safe (Atkinson, Furnell, & Phippen, 2009; Byron, 2008). Therefore it is important to educate children on how to navigate the online landscape safely.

3. Cybersecurity Education in South Africa

There exist multiple role players responsible for cybersecurity education of children, which includes government, law enforcement, parents/guardians, schools and peers (Kortjan & von Solms, 2013; de Lange & von Solms, 2012; Atkinson, Furnell, & Phippen, 2009; Becta, 2009; Miles, 2011). Statistics related to the role that parents/guardians play in cybersecurity education in SA is a point of concern. The 2014 study by UNISA surveyed 169 schools across SA where 71% of teachers believed that cybersecurity related incidents happened at school which were not reported (Kritzinger, 2014). In many cases it was found that parents or guardians are unaware of the dangers of the internet, of it they are, they feel that it would not happen to their children (Global Kids Online, 2016) (Minor Monitor, 2017). A 2015 survey indicated that parents generally were unaware of the dangers their children face, as 86.7% of parent participants believed that their child had never experienced anything that bothered them online and will not in the near future. The study states that only 31% of participants had to ask an adult's permission before using the Internet, where 46% of participants between 9 and 17 years of age could use the internet any time they wanted (Global Kids Online, 2016). These statistics show that in many cases parents are unaware of the various threats their children face and therefore the children may be uneducated on how to handle them when they do run into trouble.

The formal inclusion of cybersecurity curricula in South African schools is not a simple task as schools face challenges such as a lack of resources, experience in the field and a general lack of knowledge by teachers on the various cyber threats and corresponding safety measures (Atkinson et al., 2009; Miles, 2011; Von Solms and Von Solms, 2015). A 2014 study found that 90% of students felt that there needs to be more cybersecurity education in schools. Approximately 88% of teachers agreed that learners are exposed to Internet dangers, where inappropriate content, cyberbullying, exposure to online predators and access to personal information as stated as the most serious issues. 55% of the surveyed schools stated that they had a formal cybersecurity policy, although the primary policies only included restrictions related to cell phone and internet use. Only a small minority of schools had policies relating to cyber-bullying and no schools had a formal, clear policy on the handling of cybersecurity-related incidents which may occur (Kritzinger, 2014). In the same study, 72.8% of the teachers stated that the cybersecurity related issue was handled by themselves, although less than half of the teachers felt that they were well equipped to do so (Kritzinger, 2016). From the conducted surveys, it can be seen that teachers and parents/guardians are ill-prepared to educate learners on cybersecurity issues, especially in the case of disadvantaged schools (De Lange & Von Solms, 2012; Govender & Skea, 2015; Kritzinger, 2016).

The WolfPack report stated that SA must first focus on short-term cybersecurity initiatives before medium and long term initiatives should be pursued (Wolfpack Information Risk, 2013; Kritzinger, 2016). This proposed structure is shown in Figure 1 below. A variety of short-term awareness initiatives aimed at cybersecurity awareness exist in SA (ISC Africa, 2015). However, most of these campaigns are web-based which offers little printed material, and in many cases, children do not know where or how to find information or assistance online (von Solms & von Solms, 2014; ENISA, 2010; Kritzinger, 2016). Research supports the notion that a country with a limited cybersecurity culture, the initial awareness-raising phase must involve more than a website presence to create awareness and knowledge (CJCP and UNICEF, 2013; Kritzinger, 2016).

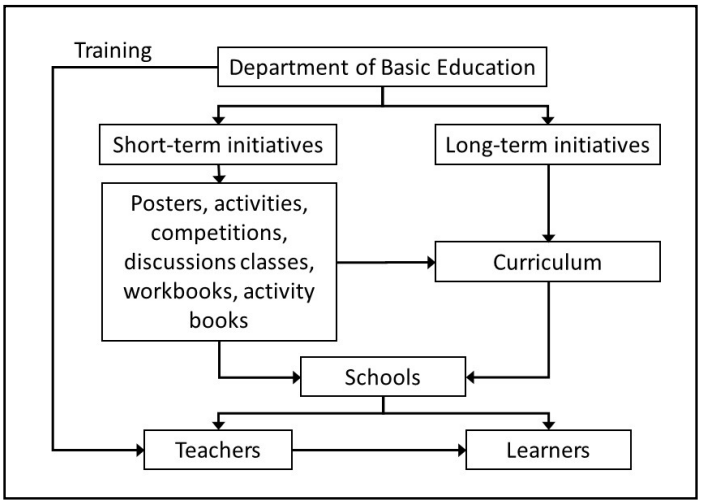


Figure 1: Long and short-term cybersecurity initiatives (Adapted from Kritzinger, 2016)

Only limited awareness campaigns exist which provides more than a website presence. The University of South Africa (Unisa), Nelson Mandela University (NMU) and the University of Johannesburg (UJ) have collaborated to form the South African Cyber Security Academic Alliance (SACSAA) (South African Cyber Security Academic Alliance, 2015). The mandate of SACSAA is to offer free education on cybersecurity, which includes informational posters and flyers as well as a curriculum for primary school learners (Von Solms and Von Solms, 2015). The African Centre of Excellence for Information Ethics (ACEIE) at the University of Pretoria provides open access material which includes a tertiary curriculum on Information Ethics to be implemented in universities across Africa, teacher's manuals and activity books for school learners relating to cybersecurity.

4. Contribution to cybersecurity education

The development of the children's book on cybersecurity, entitled Digital Well-nests: Let us play in safe nests" was developed in order to promote a cybersecurity culture amongst children. Printed books have long been the means of teaching small children how to remain safe in society. Themes like not talking to strangers or looking both ways when you cross the street can be found in libraries and book shops across the country. Just as children are taught to stay safe in the real world, they must be taught to stay safe online as well (Miles, 2011; Von Solms and Von Solms, 2015). The cybersecurity content currently available online is mainly of international origin. Online videos shows pirates or robots providing information on an issue in an English accent which is difficult to follow by a young child whose native language is not English. The use of academic terminology in the field of cybersecurity makes the core concepts inaccessible to the majority of users, including children.

The developed book contains simple explanations for new concepts and uses animals as the main characters, which are familiar to African children in general. During the developmental stages of this book, it was presented at a localisation workshop in Nairobi, Kenya in 2015 where all participants in this workshop, including academia and civil society, proclaimed that the book with its clear approach, identifiable characters and aim towards cybersecurity education, is more than sufficient to achieving the aims of localisation.

5. Overview of Book

The book is made available for free download by ACEIE as part of their open access library and is published under a Creative Commons license. The book is available for download in full colour as well as black and white outline, which serves as a cheaper alternative for schools and a colouring activity for the children. The book contains drawings on all the pages in order to keep the interest of the child. The characters in the book are all animals which a South African child will be familiar with, like a bird, rabbit, hippo or monkey. Figure 2 below shows an example of the interaction of animals with technology.

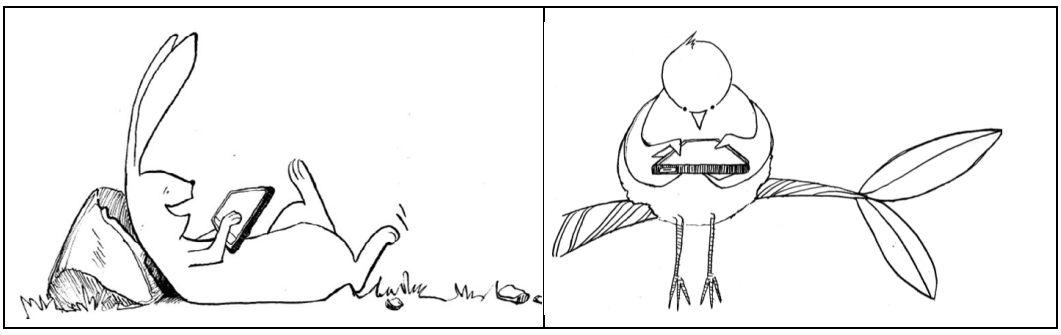


Figure 2: Illustration of animal characters interacting with technology

The book consists mainly of four sections. The first section provides a foreword to the book and is aimed at the parent/teacher/guardian, this section provides an

overview of the book and explains how the other sections can be used for best results. The three other sections include the definitions of technology-related concepts, the stories of animals relating to cybersecurity with a short moral lessons and finally a collection of short messages which can be memorised by a child. These sections are discussed subsequently.

5.1 Concepts

The book was developed with children in mind whose native language may not be English. Although the book is in English, all technical concepts are explained in this section, which includes a drawn picture or icon so that the child can identify it and point it out in the stories. The explained concepts include technology, such as a cell phone, camera and tablet, or more abstract concepts such as email and social media. Figure 3 below shows an example of the explanation of a tablet and cell phone.

Tablet		Mobile device with same functions as a computer, cell phone and e-book reader and is touch-screen. Is bigger than a cell phone but smaller than a computer and has more uses than an e-book reader.
Cell phone		Mobile device that is used to contact other people, by either phoning, texting or e-mailing.

Figure 3: Illustration of concepts and its descriptions

5.2 Poems

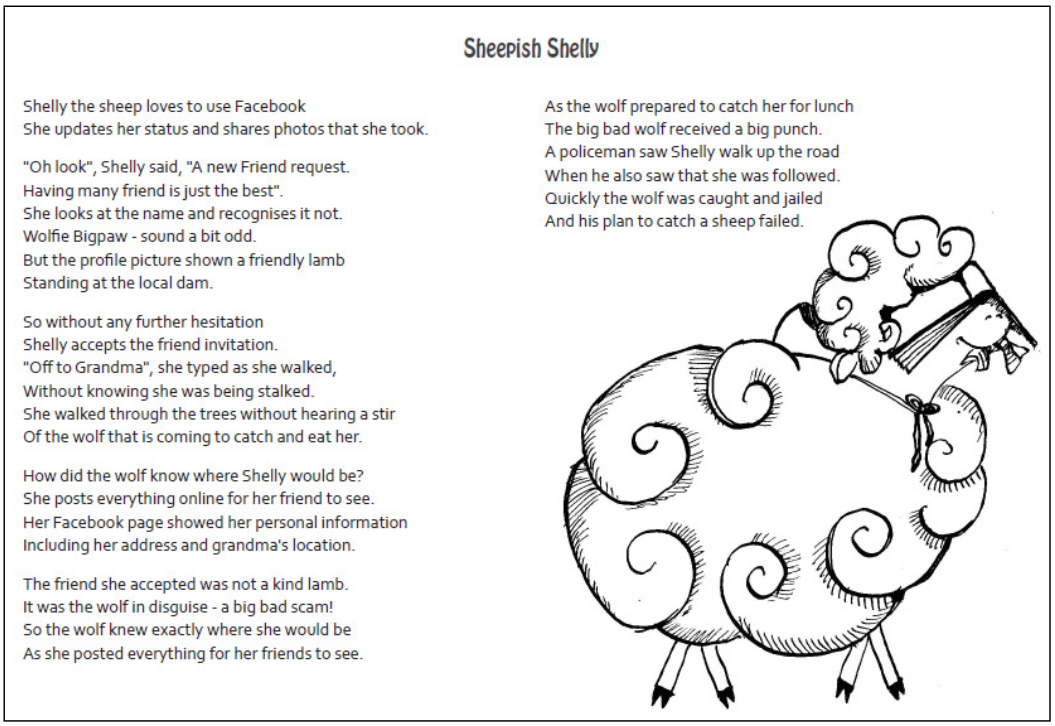
The main body of the book consists of 14 poems, each with its own story and moral lesson at the end. The moral lesson also contains one or two questions which a child can answer. These questions can be used to test the reader's understanding of technology, such as "What is an application (app)?" and "What is Google?" Other questions test the reader's understanding of the implications of technology and the importance of staying safe, such as "What are the positive aspects of the internet?", "Why is it healthy to be outside with friends and family?" and "Why is online bullying just as hurtful as physical bullying?" The names of the poems, the cybersecurity-related theme as well as the moral lesson of each is provided in the table below.

Name	Cybersecurity-related theme	Moral lesson
The safety of nests	A little bird who uses the Internet regularly listens to the guidance of his parent /teacher when using the Internet and honestly shares his experiences with them.	The internet is full of exciting opportunities, be honest when using it.
Safety Snail's e-mails	A snail who got an email from a stranger did not open it and deleted the email.	Do not open unknown or suspicious e-mails or messages.
Lucky the Fish	A fish received a text message stating that he has won a prize. He wanted to click on a suspicious link in response, but was advised by a friend to delete it instead.	Do not access or respond to unknown and suspicious messages.
Rabbit with the tablet	A rabbit and his friends visited unsafe websites on her tablet which scared her. She realised that she must be careful when online.	Be careful and safe when visiting online websites.
Elephant and his shoe	Rabbit helps his friend Elephant to search for helpful information online, but also advises him to go outside and play.	The internet is very useful, but it is just as healthy to play outside with friends!
Sheepish Shelly	A sheep accepted a Facebook friend request from somebody she did not know. She posted very personal information about herself and was followed by a wolf with a fake profile.	Only accept friend requests from people you know.
Wolf, Hyena and Fox	A fox tells his friends to create strong passwords and not to share them with anybody.	Make sure your password are strong and not easy to guess.
Healthy Bear	A bear did not update his anti-virus and his computer was infected with a virus. His father tells him that anti-virus keeps his computer safe.	Update your anti-virus programme on phone and laptop to keep them safe.
Happy Hippo	A hippo was sent cruel text messages and did not want to tell anybody as the bully was not physically hurting him. His friend the rhino convinced him that cyber bullying is real bullying and that they must tell the teacher.	When you are being bullied or see someone is being bullied, tell someone you trust.
Buffy the Bully	A buffalo feels alone and sad. He sends cruel messages to his classmates online. His teacher tells him that he must speak about his problems, as bullying is not the answer.	When you see someone is a bully, tell an adult whom you trust.
Identity Cricket	A cricket wants to make friends and posts all his personal information online. He attracts dangerous animals, not friends.	Don't make personal information available online for all to see.
Cyber Cat	A cat uses his computer skills to steal money and gain illegal access to sites. He is caught and goes to jail.	Hacking is an example of illegal online activities, there are consequences for illegal actions.
Cannot see Chameleon	A chameleon protects his identity when online by not revealing his personal information. This way he stays safe and protected.	Protect yourself when you are connected to and using the internet.
Zebra and his stripes	Zebra lines reminds you to look both ways when crossing a street so that you stay safe. Imagine zebra lines when online – stop and think before you post so that you can stay safe.	Think before your post anything on social media.

Table 1: Short description of poems and lesson

Figure 4 below shows an example of one of the poems "Sheepish Shelly" which educates children to only accept friend requests from people that they know in real life. The questions added to the end of the poem includes:

- What are better and safer ways for Shelly to communicate with her friends and family?
- What can Shelly do to improve her safety when she places notices online?



Sheepish Shelly

Shelly the sheep loves to use Facebook
She updates her status and shares photos that she took.

"Oh look", Shelly said, "A new Friend request.
Having many friend is just the best".
She looks at the name and recognises it not.
Wolfie Bigpaw - sound a bit odd.
But the profile picture shown a friendly lamb
Standing at the local dam.

So without any further hesitation
Shelly accepts the friend invitation.
"Off to Grandma", she typed as she walked,
Without knowing she was being stalked.
She walked through the trees without hearing a stir
Of the wolf that is coming to catch and eat her.

How did the wolf know where Shelly would be?
She posts everything online for her friend to see.
Her Facebook page showed her personal information
Including her address and grandma's location.

The friend she accepted was not a kind lamb.
It was the wolf in disguise - a big bad scam!
So the wolf knew exactly where she would be
As she posted everything for her friends to see.

As the wolf prepared to catch her for lunch
The big bad wolf received a big punch.
A policeman saw Shelly walk up the road
When he also saw that she was followed.
Quickly the wolf was caught and jailed
And his plan to catch a sheep failed.

Figure 4: Example of a poem with matching illustration

5.3 Short messages

The 14 short messages at the end of the book is created so that a child can memorise them. It is designed to be fun, but to also contain an important cybersecurity-related lesson to remember. These messages roughly match the lessons conveyed though the stories told in the Poems section. These can be easily memorised by children and relates to everyday encounters of cybersecurity issues, such as password protection, accepting friends online and cyberbullying. For example, in "Elephant and his shoe" tells the reader that it is healthy to also play outside. One short poem, shown in Table 2, reiterates this message. The poem "Sheepish Shelly" shows that it is dangerous to post personal information inline. Another short message confirm this, shown below.

When I play on my computer or phone. I play for an hour then leave it alone. I go outside and play in the sun. It is healthier and much more fun.	Always, always be aware That somewhere out there, anywhere. A stranger can see what you share. So always, always be aware.

Table 2: Examples of short messages from animals

6. Conclusion

In developing countries such as South Africa, children are often leading the digital uptake. This means that they are more likely to be exposed to the dangers of the internet and various negative experiences, impairing their ability to use technology to their full advantage. For this reason, children must be educated to use technology safely. As there are no formalised cybersecurity curricula in basic education in South Africa, the ACEIE sought to create the Digital Wellness toolkit to address this gap. The success of the Digital Wellness toolkit awareness-raising projects across countries in Africa emphasises the need to formally incorporate the content in the basic education curriculum. To ensure the applicability of this curriculum it remains imperative for academia and industry to run short-term initiatives to create cybersecurity awareness amongst children. Future work includes an evaluation on the book's effectiveness, including determining if the book assisted children to engage in better cyber security behaviours.

This paper presents a children's book, entitled "Digital Well-nests: Let us play in safe nests" designed to teach children about the dangers and advantages of the online world and how to stay safe when online. This book contains 14 poems telling stories of animals and their experiences with technology and the impact on their lives. The book is freely available from an open access library to assist in the cybersecurity education of small children in South Africa.

7. Acknowledgements

This work was made possible by The African Centre of Excellence for Information Ethics. The discussed book is available for download at http://www.up.ac.za/african-centre-of-excellence-for-information-ethics

8. References

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

Becta. (2009). "AUPs in context: Establishing safe and responsible online behaviours, "available online from: http://education.qld.gov.au/studentservices/behaviour/qsaav/docs/establishing-saferesponsible-online-behaviours.pdf, Accessed on [10 November 2013].

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 and UNICEF (2013), "CONNECTED DOT COM: Young People's Navigation of Online Risks", UNICEF South Africa.

De Lange, M., von Solms, R. (2012). "An e-Safety Educational Framework in South Africa," Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC).

ENISA. (2010), "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

Ericsson (2016), "Ericsson Mobility Report". doi:10.3103/S0005105510050031

Fischer (2016), "A visual representation of key terms concerns relating to cyber safety for children". https://issuu.com/universityofpretoria/docs/innovate_11_2016_high_res?e= 19359966/ 41017608 (accessed 1.1917)

Global Kids Online (2016) "South African Kids Online: Barriers, opportunities & risks".

Google (2017), "Make safety choices that fit your family" [WWW Document]. URL http://www.google.co.za/safetycenter/families/start/ (accessed 8.14.17).

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.

Kortjan, N., and von Solms, R. (2013). "Cyber Security Education in Developing Countries: A South African Perspective," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 119, pp. 289-297, 2013.

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

Kritzinger, E. (2015), "Cyber Security Awareness and Education Research".

Kritzinger, E. (2014), "Cyber Safety: A South African perspective".

Miles, D. (2011), "Youth protection: Digital citizenship — Principles & new resources", 2011 Second Worldwide Cybersecurity Summit (WCS). pp. 1–3.

Minor Monitor (2017). [WWW Document]. Internet Control Safety Tips. URL http://www.minormonitor.com/resource/internet-control-and-safety-tips/ (accessed 7.19.17).

South African Broadcasting Corporation, The Henry J. Kaiser Family Foundation, (2007), "Young South Africans, broadcast media, and HIV/AIDS awareness: results of a national survey".

South African Cyber Security Academic Alliance (2015), "SACSAA". [WWW Document]. URL http://www.cyberaware.org.za/ (accessed 8.14.17).

TeleGeography (2013), "Africa's international bandwidth growth to lead the world". [WWW Document]. Africa's Int. bandwidth growth to lead world. URL https://www.telegeography.com/products/commsupdate/articles/2013/10/31/africas-international-bandwidth-growth-to-lead-the-world/ (accessed 8.14.17).

Unicef, (2012), "South African mobile generation Study on South African young people on mobiles", Study on South African young people on mobiles. doi:http://www.unicef.org/southafrica/SAF_resources_mobilegeneration.pdf

Unicef, South Africa (2016), "South African Kids Online: A glimpse into children's internet use and online activities". [WWW Document]. Agenda. URL https://www.unicef.org/southafrica/media_18732.html (accessed 7.4.17).

Unisa (2017), "Cyber Security Awareness". [WWW Document]. URL http://eagle.unisa.ac.za/elmarie/ (accessed 8.14.17).

University of Pretoria (2017), "African Centre of Excellence for Information Ethics". [WWW Document]. African Cent. Excell. Inf. Ethics. URL http://www.up.ac.za/en/african-centre-of-excellence-for-information-ethics (accessed 8.14.17).

Von Solms, R., Von Solms, S. (2015), "Cyber safety education in developing countries". IMSCI 2015 – Proceedings of the International Multi-Conference Social. Cybernetics and Informatics. 13, 173–178.

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

We are Social and Hootsuite (2017), "Digital in 2017: Southern Africa". [WWW Document]. 2017. URL https://www.slideshare.net/wearesocialsg/digital-in-2017-southern-africa (accessed 8.14.17).

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-threatbarometer/

Zeeko (2017), "Internet Safety Guide", Internet Safety Guide.