Cyber Safety for School Children

Johan Van Niekerk, Kerry-Lynn Thomson, Rayne Reid

Cyber Safety for School Children
A Case Study in the Nelson Mandela Metropolis

Johan van Niekerk, Kerry-Lynn Thomson and Rayne Reid

Nelson Mandela Metropolitan University
Johan.VanNiekerk@nmmu.ac.za, Kerry-Lynn.Thomson@nmmu.ac.za,
s208045820@live.nmmu.ac.za

Abstract. Protecting the youth against the dangers posed by cyber space has become a matter of national priority. Parents often lack the necessary cyberspace know-how, to teach their own children how to be safe online. It has thus become the responsibility of society at large to educate the youth. This paper reports on a cyber safety poster creation campaign in the Nelson Mandela Metropolis in South Africa.

1 Introduction

For many nations, protecting the youth whilst they use cyber space, has become a matter of national importance. The UK National Cyber Security Strategy [1, p. 26] lists "tackle cyber crimes like online bullying..." as one of its "priorities for action". Klimburg [2] provides an overview of more than 20 National Cyber Security Strategies (NCSS), and notes that "Cyber security at the national level will fail when there is an inappropriate level of cyber security awareness and education" [2, p. 133]. Such awareness and educational campaigns should include all members of society and should range from primary and secondary school level, to awareness campaigns aimed at adults and the elderly [2].

The protection of national interests in cyber space has received a lot of focus in recent years. More than half of the NCSS examined in Klimburg [2] were introduced since the start of 2011. In fact, the international standard ISO/IEC 27032 [3], which differentiates cyber security from other forms of security, was first published in 2012. To a large extent, this urgency to address cyber security related issues stems from the speed with which the use of the World Wide Web has diffused through society.

The system that makes the World Wide Web possible was first created by Berners-Lee in 1990 and the first Web server became operational in 1991 [4]. Today, barely two decades later, an estimated 2.4 billion people uses the Web on a regular basis [5]. Use of the Web has permeated every aspect of many people's daily lives. The Web is used to play games, to do research, to conduct business, to perform personal financial transactions, and for many other daily tasks. Unfortunately the adoption and diffusion of many technological innovations often has undesirable and unanticipated consequences [6]. One such consequence is that the parents of the current generation of children mostly grew up before the Web

existed. These parents are thus ill equipped to teach their children how to use the Web safely. It has thus become the responsibility of society at large to try to create awareness amongst children regarding the dangers posed by cyberspace.

This paper presents a case study of a cyber safety awareness campaign conducted amongst school children in the Nelson Mandela Metropolis. The researchers hosted a cyber safety awareness poster creation competition as part of a larger national cyber security awareness week. This paper presents the lessons learned during this campaign and also discusses some interesting observations made by the researchers during the campaign.

2 Methodology

The paper is structured according to the guidelines for a Case Study as presented by Creswell [7]. Creswell suggests the following structure:

- Entry vignette
- Introduction
- Description of the case and its context
- Development of issues
- Detail about the selected issues
- Assertions
- Closing vignette

In the context of this paper, the abstract and introduction to the paper respectively serves as the case study's entry vignette and introduction. The next section will describe the case and its context.

3 Description of the case and its context

The South African Cyber Security Academic Alliance (SACSAA) was formed in 2011 by researchers from three South African universities, namely the University of Johannesburg (UJ), the University of South Africa (UNISA), and the Nelson Mandela Metropolitan University (NMMU). "The main objective of SACSAA is to campaign for the effective delivery of Cyber Security Awareness throughout South Africa to all groupings of the population" [8].

As part of its cyber security awareness activities, SACSAA hosted South Africa's first national cyber security week in October 2012. Preparations for this first national cyber security awareness week started in 2011. The initial plan was to host such a week in 2011. However, due to logistical reasons it was decided to postpone the first national week to 2012. Each of the three founding institutions committed to conducting at least one major cyber security awareness initiative as part of the activities for this national event. The NMMU researchers decided to host a cyber security awareness poster creation competition. This poster competition forms the focus of this case study. The case study will present a brief overview of the hosting of this competition and will report on the lessons learned by the researchers conducting this event.

4 Development of issues

A 'trial run' of the planned poster creation competition was held in 2011. This was followed in 2012 by the first fully fledged competition. The following subsections will briefly describe how the hosting of the 'trial run' differed from the first fully fledged awareness competition in 2012.

4.1 The 'trial run' in 2011

The 2011 'trial run' started in the 3rd term of 2011. During this term hundreds of professionally created and printed promotional flyers, which advertised the competition, were distributed via 'snail mail' to schools in the Nelson Mandela Metropolis. Flyers were also posted on noticeboards across the NMMU campus. Figure 1a shows an example of the 2011 competition flyer.

(a) Competition Advertising Flyer

(b) Cyber Safety Pledge

Fig. 1: Examples of material distributed to schools.

The 2011 'trial run' called for entries in the form of either awareness raising posters or videos. The posters could be submitted in either digital form or physical copies could be mailed as entries. The competition asked for entries in one of three categories, namely:

- A primary school division
- A secondary school division
- An open school division, which anyone could enter, irrespective of age

The competition offered cash prizes to the winners. These prizes were reasonably generous in the South African context.

Despite a lot of effort in the advertising of the contest during this year, only three posters and one video were received as entries for this 'trial run' competition.

4.2 The first 'official' competition in 2012

In 2012 the first 'official' competition was hosted as part of the national cyber security awareness week. A lot of effort went towards not repeating the mistakes that were made during the previous year's 'trial run' competition. The following changes were made:

- Flyers to call for participation in the competition was printed during the first term of the year and immediately distributed. This was done because many school teachers who received flyers via the mail the previous year responded with concern that the third term was too late in the year for them to meaningfully encourage learners to participate.
- The competition was more focused. Only poster entries was called for and the previous year's video category was removed.
- Entries were restricted to the school children only. There was thus just a primary school and secondary school division call. The previous year's open division was removed because the researchers felt that this category did not meaningfully contribute to the actual raising of awareness amongst the entrants.
- The researchers visited several schools and delivered competition flyers in person. Whilst delivering these flyers effort was made to explain the context and purpose of the competition to the teachers involved.
- Following the hand delivery of competition flyers the researchers were invited to present cyber security talks at some schools. During these talks copies of an awareness flyer developed by the researchers entitled "Cyber Safety 101" were distributed to teachers and participating learners. These awareness flyers are discussed in depth in a later section.
- The competition received radio and media exposure as part of the larger national cyber security awareness week campaign. Following this exposure, many sets of competition flyers and accompanying basic awareness flyers were distributed on request to schools in several provinces.
- The competition was supported by the activities of other SACSAA member institutions. Of specific interest to this case is the distribution of a cyber security pledge form to learners in participating schools. This pledge form was signed by learners and signified that they pledge to 'surf on the safe side'. The pledge form listed three promises which all reinforced specific messages that also formed part of the messages on the "Cyber Safety 101" flyers. The pledge form and other awareness material distributed as part of the larger national campaign were branded with a 'mascot' in the form of a robot figure with a lock on its chest. The pledge form is depicted in Figure 1b.

The 2012 campaign had considerably more participants that the trial run in 2011. A total of 217 poster entries were received. Of these entries 94 were from

primary school children and 123 were from secondary school children. However, despite having many requests from schools located all across South Africa for competition flyers, educational material and additional information regarding how to enter, all entries received were from the Nelson Mandela Metropolis. In fact, all entries were received from schools that were visited in person by a member of the research team to advertise the competition and explain its purpose to learners and teachers.

The following section will provide more detail regarding the awareness message given during our visits at schools and will present the results of a content analysis performed on the poster entries received.

5 Detail of selected issues

5.1 Educational Flyer

During the initial 'trial run' in 2011 many teachers who were asked to encourage their learners to participate stated that they did not know enough about cyber safety and/or security to give advice to children regarding poster topics. This lead to the creation of an educational flyer by the researchers which were send to schools with the 2012 poster contest flyer. The flyer lists seven basic cyber safety 'rules' that children can follow to help them stay safe online. The contents of this flyer also formed the basis of the cyber safety talks presented at the schools by the researchers.

The following is a verbatim copy of the listed 'rules' on this flyer:

1. Protect your computer - As a minimum every computer should run an antivirus program and a firewall. Very good antivirus and firewall software is available free of charge. Visit our website for more info.
2. Have a good password - A good password should contain UPPER and lower case alphabetic characters, numbers, and some special characters. Try using the first letter of every word in a sentence combined with a few twists like using the last word in full. For example: My name is Bob and I like to eat = MniBaIl2e@t.
3. Never share personal details online - One of the biggest online dangers is that criminals can find your personal information like your ID number, date of birth, address, or cell number and use it to steal your identity. Never post either your own, or anyone elses personal information online!
4. Dont trust anyone online - People you meet online are rarely who they say they are. Never believe that someone you met online is telling you the truth. Be especially wary of gifts, competitions, and other prizes. How can you win if you never entered?
5. Dont break the law - Illegal software, games, or music often contains hidden malware. Why would someone go through all the effort to crack the copy protection on a file if there is nothing in it for them?
6. Dont be a bully - Everything you post online stays there forever, even if you delete it. Do you really want the people you are going to work for one day to know how nasty you were to someone else today?

7. Trust someone - It is a good idea to have at least one adult you can trust who knows who you are talking to online and what you do when you are online. This could be a parent, uncle, aunt, teacher, or even a brother or sister.

The above mentioned flyer was handed out at all schools that were visited in person during 2012. Schools that requested that additional information be mailed to them via 'snail mail' also received copies of these flyers. Due to available time and logistical issues, schools that were initially visited and invited to participate did not receive copies of these flyers unless they were also visited a second time for the researchers to present a cyber safety talk to the learners.

5.2 An Analysis of the Poster Entries

All 217 poster entries in the 2012 competition came from only four schools, one was a primary school with most learners between the ages of 6 and 13 years of age. The remaining three were secondary schools with learners predominantly aged between 13 and 18 years old. All of these schools were amongst those visited in person by the researchers. However, only the primary school received a cyber safety talk and the accompanying copies of the "Cyber Safety 101" flyers. In all cases the researchers were contacted by the teachers of the entrants and asked to collect the poster entries for the entire school in a batch. The primary school children thus each had a copy of the topics suggested by this flyer, whilst the secondary school children's entries were primarily based on their own, or possibly their teacher's, perceptions of what would be relevant topics.

The authors performed a qualitative content analysis on all the poster entries that were received. For this analysis the following questions were asked for each poster:

1. What topic(s) is covered by the message(s) in the poster?
2. Is the poster specific to one category (form factor) of device?
3. How well has the cyber safety message been internalized (in the researchers opinion)?

Each of the above questions will be briefly elaborated on in the following sub-sections.

Posters per Topic This question was asked to firstly determine how well the message contained in the 'Cyber Safety 101' flyer was received by the learners. Secondly the researchers wanted to know which specific topic(s) was seen as more important by the learners and whether or not there was a difference between the topics primary school children and secondary school children considered important. Figure 2 shows the results of this part of the analysis. As can be seen in Figure 2 the primary school children predominantly based their posters on messages contained in the "Cyber Safety 101" flyer, whilst the secondary school entries also included the topics of social networking, phishing, and identity theft.

Secondary school entries on the "Protect your computer" topic also covered a much wider range of malware and were not restricted to anti-virus or firewall related messages, while most primary school entries were restricted to topics on the educational flyer. Of interest to the researchers was that the most popular messages for primary school children were to not trust strangers, or give out personal information online. For secondary school learners the most popular message by far was not to be a cyber-bully. Very few children chose the message that related to not using illegal software or media as the topic for their posters.

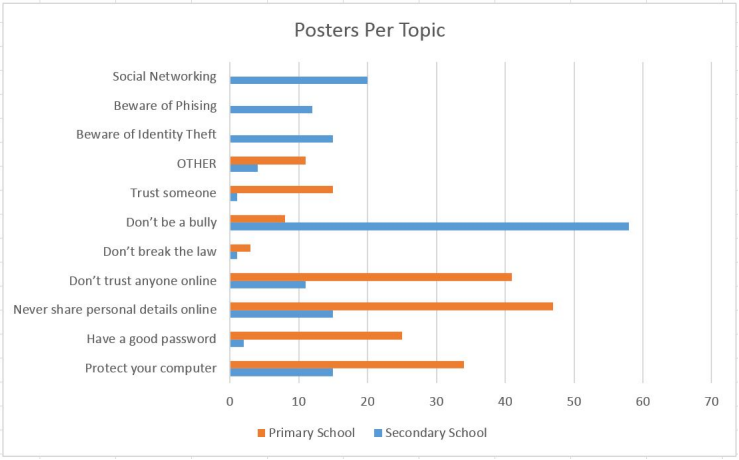

Fig. 2: Number of Posters per Topic

Also of interest to the researchers was that many (20 out of 94) of the primary school posters used the robot 'mascot' in the poster design. In many cases where the robot was used, the message stated that the robot will help protect you against the dangers of cyber space.

Posters per Category of Device The purpose of this question was to determine whether the children associated the Web with a more 'traditional' computer, or with a mobile device, or whether they made no distinction between computers and mobile devices like smart-phones. The results of this analysis is shown in Figure 3. From this analysis it appears that the primary school children tend to associate Web use with a single device whilst secondary school children do not make such a distinction.

Internalization of Cyber Safety Message The final question asked in the analysis attempted to judge how well the child internalized the message(s) portrayed in the posters. If the poster just re-iterated a message from the flyer in more or less the same words as it were given to them it was rated as "As given".

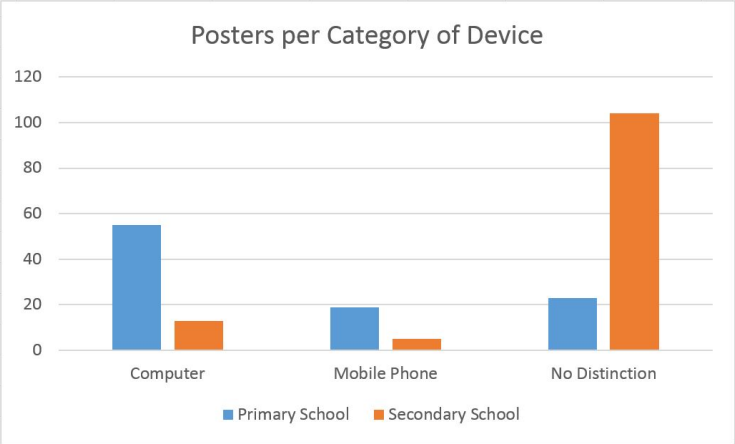

Fig. 3: Number of Posters per Category of Device

If however the message was expressed in the child's own terms it was rated as "Rephrased in own terms". Finally if there was clear evidence that the child also understood the implications and/or consequences of not adhering to the message's advice it was rated as "Fully internalized". An example of a poster considered "Fully internalized" is depicted in Figure 4. In the poster shown in Figure 4 one can clearly see how the child interpreted the concept of cyber-bullying. A character called Sam sent an untrue message claiming "Jo said she likes Mike". Jo is crying because she never said this and Mike is confused because he was unaware that Jo likes (has a crush on) him. The poster shows that the child understood false messages about others to be cyber-bullying; she also understood that such action could hurt others, hence Jo's tears, and by showing the same message on all depicted character's devices she demonstrated that she understands that such bullying is often via a public forum and not limited to one-on-one communication.

An initial analysis compared primary to secondary school children. However, it was found that almost all the secondary school entries were rated as "Fully internalized". The primary school sample was then sub-divided into children aged 6 to 9, and those aged 10 to 13 for a secondary analysis. This analysis, as depicted in Figure 5 showed that the younger children internalized the safety messages to a lesser degree than the older group.

6 Lessons Learned

During the 2012 poster competition the researchers have learned many lessons, which can hopefully assist in making similar campaigns in future more successful. The following is a brief summary of the lessons learned:

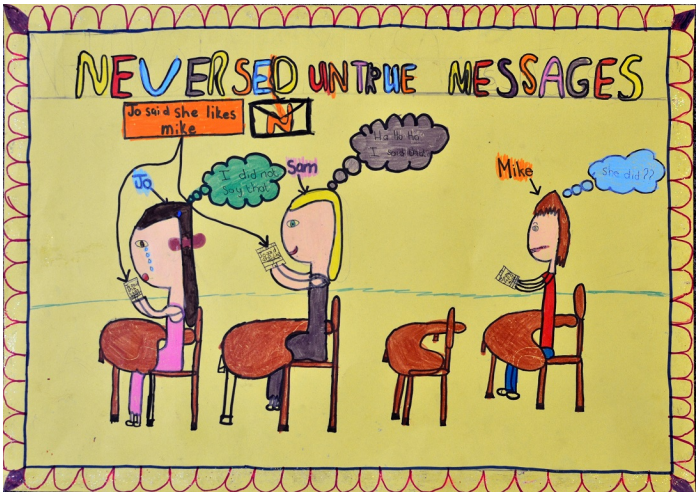

Fig. 4: Example of internalized poster

1. Schools will only participate in campaigns like these if they are notified of the campaign early in the school year.
2. Personal visits to schools are a lot more effective than mailed invitations. No entries were received from schools that were not visited in person. Even schools that specifically requested entry information via the mail did not participate.
3. Teachers play a vital role in such campaigns and need to understand the relevance of the campaign.
4. Prizes should be distributed across many categories. Initially the researchers planned to have prizes split into only two categories, namely primary and secondary school categories. However, many primary school teachers expressed concerns that it would not be fair to judge/compare poster entries by 6 year olds against those entered by 13 year olds.
5. Guidance regarding judging criteria should be specific enough to ensure desired outcomes. The intention of the poster creation campaign was to use the best poster entries received as awareness raising posters in future campaigns. Unfortunately a lot of the entries had a lot of text and were in the format of informational brochures, rather than that of awareness posters.
6. Mascots and other branding should be chosen with care. Children do relate the mascots to the topic.
7. Hand drawn or painted entries should be encouraged. The majority of entries that were created with the aid of a computer were of a 'cut and paste' nature. The researchers believe that the hand drawn posters provided a better indication of actual assimilation of the subject matter.

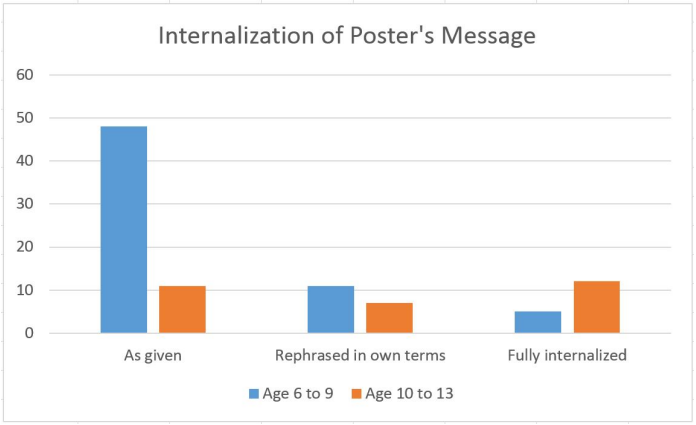

Fig. 5: Internalization of poster's message.

7 Conclusion

Protecting the youth in cyber space has become the responsibility of society at large. Without an appropriate level of cyber security awareness and education national cyber security strategies cannot work. This paper reported on a cyber safety awareness campaign conducted in the Nelson Mandela Metropolis in South Africa. The paper described how a poster creation campaign was used to raise awareness about cyber safety related issues amongst both primary and secondary school children. The paper briefly presented the researcher's observations during this campaign and some lessons learned which could help contribute towards the success of future campaigns.

References

[1] Minister for the Cabinet Office and Paymaster General: The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. (2011)
[2] Klimburg, A., ed.: National Cyber Security Framework Manual. NATO CCD COE Publications, December 2012 (2012)
[3] International Standards Organization: ISO/IEC 27032:2012(E) Information technology - Security techniques - Guidelines for cybersecurity (2012)
[4] Chen, H., Crowston, K.: Comparative diffusion of the telephone and the World Wide Web: An Analysis of rates of adoption. In Lobodzinski, S., Tomek, I., eds.: Proceedings of the WebNet '97 World Conference of the WWW, Internet and Intranet, Association for the Advancement of Computing in Education (1997) 3–7
[5] www.internetworldstats.com: World internet users and population stats
[6] Rogers, E.M.: Diffusion of Innovations, 5th Edition. Simon and Schuster (2003)
[7] Creswell, J.W.: Qualitative inquiry and research design: Choosing among five approaches, (2nd Edition). Thousand Oaks, CA: Sage (2007)
[8] SACSAA: South african cyber security academic alliance. http://www.cyberaware.org.za