Towards a cyber security aware rural community

Prof Marthie Grobler
DPSS, CSIR
Pretoria, South Africa
mgrobler1@csir.co.za

Zama Dlamini
DPSS, CSIR
Pretoria, South Africa
idlamini@csir.co.za

Sipho Ngobeni
DPSS, CSIR
Pretoria, South Africa
ngobeni@csir.co.za

Aubrey Labuschagne
DPSS, CSIR
Pretoria, South Africa
wlabuschagne@csir.co.za

Abstract— **A large portion of the South African rural community only have intermittent access to computers and are not familiar, nor entirely comfortable, with the use of internet communication or electronic devices. The research conducted by the authors of this paper confirms that this lack of awareness, combined with the inherent dangers posed by the internet, expose local communities to cyber threats. Especially rural communities are not always empowered to deal with these threats.**

In an effort to prevent innocent internet users from becoming victims of cyber attacks, a cyber security awareness campaign is developed to educate novice internet and technology users with regard to basic cyber security. The motivation for this awareness project is to educate all South Africans on the safe use of the internet, in an attempt to strengthen the cyber security awareness level concerning the South African network. The hypothesis is that if there are local communities that are not properly educated, their technology devices may remain unprotected. This may leave the South African internet infrastructure vulnerable to attacks, posing a severe threat to national security and eventually affecting communities other than those directly involved.

This research paper focuses on promoting cyber security awareness towards the newly released broadband capability and knowledge transfer within rural communities by means of a voluntary community based training program. This program can be adapted in any environment other than rural communities, but the current focus has been in the rural areas. The program takes on an informal work session approach with presentations and discussion sessions. The cyber security awareness program modules are divided into four main themes: physical security, malware and malware countermeasures, safe surfing and social aspects of cyber security.

These themes are developed in such a way to cover a wide range of topics, including practical advice on phishing attack avoidance and more advanced topics such as preventing social engineering attacks. This paper will introduce the development of the cyber security awareness program, and emphasize the importance for including these specific themes at the hand of international cyber security incidents.

Keywords-component; cyber security; awareness; South African rural communities

I. INTRODUCTION

In an effort to prevent innocent internet users from becoming victims of cyber attacks, the Council for Scientific and Industrial Research (CSIR) has initiated an intensive cyber security awareness program developed specifically to educate novice internet and technology users with regard to basic cyber security. This paper uses the inbuilt dangers posed by the internet, as well as the limited exposure to online activities in the South African rural areas to identify and build towards a program for a cyber security aware rural community.

Since rural communities are not always empowered to deal with cyber related threats, this is a potential weakness that can expose local communities to cyber threats. This research focuses on promoting cyber security awareness towards the newly released broadband capability and knowledge transfer within rural communities by means of a voluntary community based training program [9].

The target audience for this program is computer users with working computer literacy and awareness and prior exposure to the internet. These individuals should not have any formal computer related training, with the exception of computer literacy courses. For the time being, four user groups are identified:

- secondary school pupils,
- further education training (FET) college students,
- university students not studying towards a technical or information technology degree, and
- community members using the computer facilities of community centers.

The program is rolled-out in the Vhembe District, Thohoyandou in the Limpopo province of South Africa. Within the province, entities had to be selected to partake in this program. For the initial training program, only schools and centers that have previous exposure to computer facilities and internet access are selected as participants in the setup.

II. MOTIVATION FOR THE AWARENESS PROJECT

Over the past number of years, the internet has evolved tremendously [22]. This is evident from the fact that, today, a large number of people use the Internet for business, education, banking, and even for social purposes. This revolutionary technology provides some convenience; however, it possesses a dark side in the form of security threats. It is, thus, crucial that security initiatives are undertaken to educate cyber users.

According to McAfee Avert Labs, approximately 200 new types of malware are created everyday, with Social Networking (SN) sites becoming the newest targets of computer malware creatures [12]. At the beginning of 2011, Norton reported that the top five cyber threats require the interaction of the internet user [10]. These threats includes: social media identity theft, smartphone and table hacking, trending topics, shortened web addresses and pharming. This means that cybercriminals have

Acknowledgement must be given to the Council for Scientific and Industrial Research (CSIR) and the University of Venda for their financial support on this project.

moved away from the random type of attacks to more organized and sophisticated methods, such as spying, plotting attacks using other people's computers, etc. This requires the digital devices' owner to be ready and aware of the current threats associated with their devices.

In 2010 alone, a computer virus breached almost 75 000 computers in 2 500 organizations around the world, this included user accounts of popular social network websites, according Internet security firm NetWitness [20]. This is only part of the motivation behind education computer users regarding cyber security.

The motivation for this awareness project is to educate all South Africans using the internet, in an attempt to strengthen the awareness level with regard to the South African network - if there are local communities that are not properly educated, their technology devices may remain unprotected. This may leave the South African internet infrastructure vulnerable to attacks, posing a severe threat to national security [9].

III. Development of Cyber Security Awareness

The inclusion of each of the four themes (Theme 1: Physical Security, Theme 2: Malware and Malware Countermeasures, Theme 3: Safe Surfing and Theme 4: Social Aspects of Cyber Security) were carefully calculated to ensure a balanced programme. Basic security measures are selected to ensure that even the person with very limited access to technology can enjoy some level of cyber security. Broad guidelines are included pertaining to safe surfing and safe email practices. This is all supplemented by an eminent emphasis on personal information protection and vigilance against online frauds, scams and tricks. Users should understand that the information provided, is shared with a diverse group of people. These people have different intentions with the information provided. Some individuals could use this information to perform a physical attack when the users provide physical location information. Information provided on social networking sites is permanent. Information is collected by the site and by other collection mechanisms which impedes on the process to remove the information shared by the users.

A. Theme 1: Physical Security

Physical security is an introductory session that provides users with a basic understanding of securing their physical digital devices (for example, personal computers, laptops and mobile phones). This training session addresses the importance of securing hardware and software access of digital devices in order to protect internet users from potential cyber security threats. This session addresses the physical protection of computers, laptops and mobile phones, as well as the importance of password protection. The main points of each of these physical security measures are discussed below.

1) Physical Computer Security

The importance of protecting digital devices is rampantly overlooked, or assumed to be understood by every device owner. Unlocked computers, storage devices that lie around, passwords written on scraps of papers and web cameras are all at the mercy of hackers. Protection should always be the users' first line of self defense.

The components of physical computer security and related physical threats to online security can be identified as follows:

- Computer tower and storage media - Users are taught the importance of safe keeping and packing away of any unused external storage media. Users are taught the significance of looking for suspicious devices that may be used by cyber criminals before they start using the computer.
- Computer monitor - Users are taught to be vigilant of pop-up messages, especially if these pop-ups pertain to 'Remote desktop' (it can be used by other people to infiltrate the computer and steal their information) [7]. An important aspect addressed in this topic is people's bad habits of sticking passwords as reminders on their monitors. Users are cautioned against this behavior.
- Workstation - Users are shown easy ways of locking the workstation without shutting it down as an important precaution against unauthorized workstation access. The importance of privacy and access control are emphasized throughout the sessions.
- Peripherals - Users are trained to look for unusual signs of a potential workstation physical security breach. These sessions touch on unusual mouse activated infrared and remote web camera activation.
- Hard copies - Dumpster diving is also addressed and users are urged to be vigilant. They are advised to protect their identity in the physical world by never throwing away letters with their personal information (such as name, address and ID number) as dumpster divers can get hold of them. Users are advised to shred all documents containing personal information before it is thrown away.

2) Physical Mobile Security

Accessing internet using mobile phones comes with the same consequences as using a computer or a laptop; therefore users are advised to apply all basic safe surfing best practices on mobile phones as well. Users are further advised to install and frequently update the mobile phone anti-virus software and other security related software as well as the mobile phone patches.

Mobile phones are more vulnerable than fixed telephones or landlines. With regard to cyber security, this may be due to:

- eavesdroppers that can listen to users' calls,
- cyber criminals that can bill their own calls using other users' accounts, and
- modern smart phones are comparable to laptops and desktop computers, especially on the internet access features.

In addition, with many of the rural community members not having regular access to an internet-connected computer, these individuals often access the internet through their mobile phones. This leaves them vulnerable to these attacks [14].

3) Password Protection

Passwords are often perceived as a hassle for users to remember, while easy-to-guess passwords are cyber criminals' main preference to gain access to users' online accounts and computer files. However, passwords are a user's defense to keep all unauthorized people from accessing their profiles.

Therefore, creation and maintenance of passwords is crucially significant. During this session, users are practically taught and assisted in techniques to ensure the creation of a secure password that would be hard for humans or computers to guess, yet easy for users to remember and easy to type. The methods that are normally used by cyber criminals to get hold of users' passwords are demonstrated on video clips and also discussed. Users are further trained on best practices for passwords. The responsibility that is expected from users on the safekeeping of their passwords is also emphasized.

B. Theme 2: Malware and Malware Countermeasures

The theme on malware and malware countermeasures touches on some of the different types of malicious software that can be encountered in cyberspace, and provide guidelines on how to protect a computer or mobile phone from these malware types. Due the rapid development of the internet, and the equal rapid development of software application with malicious intent, it is necessary to educate users on malware threats and possible countermeasures against this malware. It is therefore of vital importance for computer users to stay on the forefront of the threats posed by computer malware.

The main points of malware and malware countermeasures theme are discussed below. During these sessions, emphasis is placed on the identification of computer malware and different types of computer malware, and the identification of possible defense measures necessary to protect your computer against computer malwares.

1) Computer malware

Users are introduced to the concept of computer malware, short for malicious software and typically used as a catch-all term to refer to any software designed to cause damage to a single computer, server or computer network [14]. During this session, it is emphasized that computer malware is a software program that damages the computer system or does something unwanted to the computer, and generally include all references to computer viruses, worms, Trojan horses, backdoors, exploits, etc. [17].

Over the past several years, the goal of computer malware has shifted to a financial related motive. Instead of designing malware for electronic vandalism, they design malicious software that stealthy use infected machines to accomplish their objectives. This includes sending out spam, stealing credit card information, displaying pop-up advertisements, and providing backdoors to organizational networks [4].

Some types of malware are discussed and compared, by means of multi media support files. This session also guides users in the event that malware be identified on a computer. In addition, users are taught how to protect themselves. This includes basic guidance with regard to installing an anti-virus program, as well as general rules to apply to prevent majority of malware infections.

2) Pop-ups, adware and spyware

This session defines the meaning of pop-ups, adware and spyware. The session also looks at the dangers associated with these malwares and further points out defense measures that users can use to protect themselves against these malwares.

3) Botnets

The presentation on botnets is a rather technical presentation that explains to the users what botnets are and how they can be used by cyber criminals to infect ordinary users' computers. The session explains terminology such as bots, botnets, botmasters and zombie networks. Users are familiarized with the botnet lifecycle, botnet activities and malicious uses of botnets, such as Denial of Service (DoS) attacks, spamming, traffic monitoring, key logging, mass identity theft, botnet spreading and pay-per-click system abuse.

Possible signs of botnet infection and protection measures against botnet infection are discussed. The session concludes by looking at good security practice in order to minimize botnet infection.

C. Theme 3: Safe Surfing

The safe surfing session addresses the guidelines that internet users should practice to ensure that the time they spend online are productive and secure. This session addresses internet surfing, email security, file sharing, copyright, downloads and storing in more detail.

1) Surfing the web

This session focuses in particular on teaching users what they should and should not do to stay safe when using the internet. It is emphasized that the internet has a lot of benefits for those that know how to use it. However, there are also a number of pitfalls such as inappropriate materials or websites, downloadable and executable malware, and dishonest strangers that can pretend to be someone that they are not. This session is individualized to match the age group of the learners.

Brief guidance is given on how to block websites and mark it as restricted, and the importance of personal information privacy is emphasized. Users are taught about flaming and spamming.

2) Email security

With many communications nowadays taking place through email [6], it is necessary that users know how to properly use email. This session addresses the following main points:

- What is an email and how does it look - Users are familiarized with the layout of both application email package and web based email packages. Terms such as CC (carbon copy) and BCC (blind carbon copy) are also explained and illustrated.
- Which emails can be opened - General guidance is provided with regard to emails that may be potential spam or malware infected. Users are taught a number of tell tale signs that are often associated with potentially dangerous emails.

- After opening the email - Further guidance is provided regarding emails that have been considered safe to open. This part focuses on chain mails and downloading .exe files.
- Tips on sending good emails – This includes basic guidelines pertaining to the construction of a good subject line that will not trigger spam filters, using the spell checker, adding a signature to the end of the email, explaining the reply all function, attachment size and protecting personal privacy.

3) File sharing and copyright

Users are introduced to some of the aspects of South African law pertaining to actions on the internet. The focus of this session is on legal file sharing and the protection of copyright. The dangers of illegal file sharing and downloads are explained, from both a legal aspects as well as the potential for downloading malware.

4) Internet banking

The awareness presentation on internet banking is one of the most significant presentations in the awareness programme, since it has a potential impact on both money and personal data. This session will allow the users to understand the related security measures and will enlighten them on best practices when using internet banking.

The session briefly explains what internet banking is, the benefits of using internet banking, the risks of using internet banking as well as best practices to ensure adequate protection against majority of these risks. The most common banking frauds are discussed and users are shown how to look out for specific fraud related tell tales.

5) Phishing attack avoidance

The number and sophistication of phishing scams sent out to internet users is continuing to increase dramatically. This session shows learners what to look out for when accessing websites to avoid falling victim to phishing scams.

Phishing attacks occur when the attacker steals information that defines a personal identity (such as name, surname, identification number and credit card details). Attackers could use this information to access bank accounts or use the information to create an entity with the collected information to perform cyber crimes. Phishing attacks are often performed by using emails or SMSes (referred to as smishing) to lure users to open these emails and complete the requested information.

An example of a phishing attack is when an attacker forges an email that looks like a legitimate financial institute email requesting the user to update personal details. This type of attack could be mitigated by making users aware of phishing attacks, how to identify such an attack and what to do when the user encounters such an attack. This session guides users in identifying a secure website and to how to look for a potential phishing website.

D. Theme 4: Social Aspects of Cyber Security

Social aspects of cyber security address the safest way to use SN, as well as the dangers that are associated with social media on the internet and cyberspace. Some studies have reported on the benefits of using social networking sites. Ryan and Xenos [18] investigated the relationship between an individual's personality and the use of Facebook. This session also introduces social engineering, identity theft, cookies and cyberbullies [9].

1) Social networking

Users are introduced to different types of social networking, its benefits and advantages. SN sites are platforms created to allow people to communicate through the use of this digital platform. Users create content on these platforms by adding comments, pictures and links to websites, creating relationships with other users and creating virtual groups. According to Alexa, Facebook is the most frequented SN site [3]. In addition, a study by Shaw and Gant [19] found that the Internet reduces levels of loneliness. Facebook has been identified by Kabilan *et al.* [11] as a powerful tool to facilitate the learning of the English language.

Some of the benefits of SN sites include the potential to aid in disastrous times. For example, SN sites Facebook and Twitter were used during the earthquake relief efforts in Haiti [16]. These sites have also been used by non-profit organizations to advance the organization's mission and programs [22]. Unfortunately, cybercriminals have identified Facebook as a platform that could also be used for malicious intentions. This session focuses specifically on teaching the users how to ensure that the security and privacy settings on some of South Africa's favorite SN sites are correct. Users are made aware of the dangers of SN, and especially the importance of personal privacy is emphasized during this session.

2) Social engineering

Social engineering is the use of social disguises, cultural ploys, and psychological tricks to get computer users to assist hackers in their illegal intrusion or use of computer systems and network [1]. Social engineering tactics could easily be implemented in cyber space due to the faceless characteristic of the Internet and the number of unaware users that do not understand the dangers that are currently present.

Current research has identified a list of attacks that affect the usage of the Internet [13]. This, combined with the unpredictability of the users, provides attackers a vector for possible exploitation. Attack vectors generally consist of technical and psychological ploys to lure users to execute malware. The creators of the malware use social engineering to incite users to perform actions which infects the systems, including persuasive techniques used to lure the users [1]. These can be defined as follows: curiosity, empathy, and excitement; fear; and greed. Specific subject lines are selected that will draw the attention of the user and lure the users to open malicious email attachments.

This session introduces the users to the different stages of social engineering attacks, and provides practical examples to make users aware of the possible scenarios. An example of a successful social engineering attack pertains to the 2008 Beijing Olympic Games as context to draw curiosity from the unsuspecting user to open the malicious file that exploited and infected the system [8]. Another example of this would be the nuclear incident in Japan. Emails were created, describing the

incident to draw the attention of the user and then luring the user to open an attachment that contains the malicious payload.

3) Identity theft

Information gathered from SN sites can be potentially used for various attacks, including but not limited to identify theft, cyberbullying, social engineering, evil twin attacks and malware. SN sites are inherently designed to allow users to provide information that could be used by cyberbullies and cybercriminals. This session focuses on making users aware of the consequences of posting personal information on the internet that can be used as part of identity theft.

4) Cookies

Most access to the Internet is through the use of a web browser, which uses cookies as "a piece of information generated by the web server and stored on the users' computer, ready for future use" [15]. The cookie is used with future transaction with the web server which uniquely identifies the user.

Since cookies are often created without the consent or knowledge of the user, this session focuses on making users aware of cookies, as well as the respective benefits and disadvantages. Cookies can be used to customize the user experience by storing personal preferences but also can be used to log into a protected web site using authentication, i.e. storing usernames and passwords, credit card details, physical address and identity numbers. Although cookies are useful for the duration of the interaction with the web site, it can be employed for malicious intent. Users are made aware of this.

5) Cyberbullies

Cyberbullying can be defined as "bullying that take place outside of the usual reality of direct contact and is a method of harassment that typically involves a child, preteen, or teenager [21]". Children can make use of a digital platform to launch these attacks at other children. These messages can potentially contain death or physical threats.

This cyberharassment can be conducted by sending email, photos, instant messaging, text messages, video through cell phones, digital devices and computers [19]. Accordingly, it is crucial to teach users to recognize cyberbullying and to make them aware of the appropriate ways to respond to cyberbulling.

Cybercriminals use personal information gathered from the internet, especially from SN sites, to track down, stalk and abduct youth. These criminals can further their ploys by using the SN sites to initiate a relationship, form communication with the victim, disseminate and access information, and getting in touch with the friends of the victim.

IV. RESULTS

With more than three training sessions conducted in the Vhembe Districts, the results have been tremendously positive and inspiring. Before and after each training session, the trainees are tested on their level of understanding regarding all the themes included in the training programme. This is analysed and the results are used for further emphasis and future improvements.

Figure 1 shows an example of one of the questions that the trainees answered before receiving training.

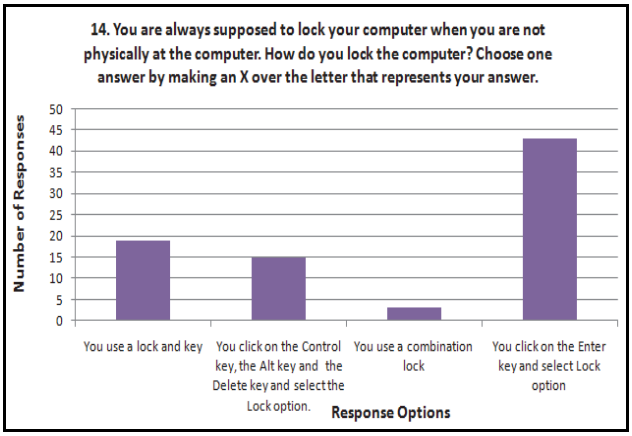

Figure 1: Multiple Choice Pre-Survey Data

Figure 2 shows an example of one of the questions that the tra

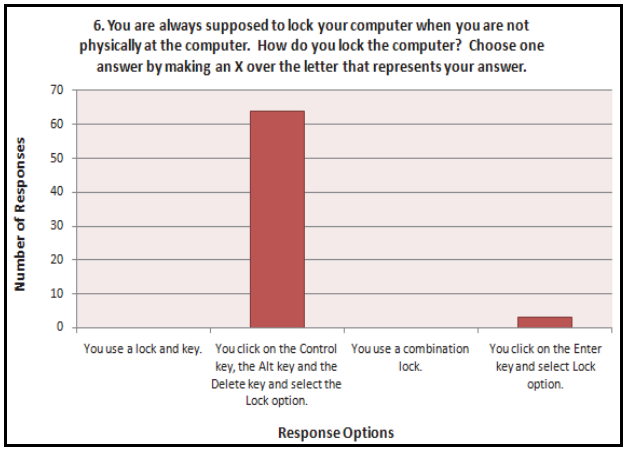

Figure 2: Multiple Choice Post-Survey Data

The example of the open-ended survey questions are shown An example of an open-ended survey question are shown in Table 1 and Table 2

.

Table 1: Open-Ended Pre-Survey Data

What is adware?
A program that is designed to weaken a computer's internet security system,
Is a type of computer worm that destroys the computer and steals information,
Adware is the software that the adversary uses to attack or harm the computer,
A computer program that are designed specifically to work with certain software,
A type of malware that penetrates a computer to damage its software,
It is software that uses an active attack to attack a computer,
A type of malware, it is the system program which functions like a virus,
Be very sure of your safety in social network,
Is software that has got a harmful impact on your computer,
Unknown.

Table 2. Open-Ended Post-Survey Data

What is adware?
Program which gives advertisements illegally,
A computer program that show adverts to a user in a form of pop ups which are annoying,
Is a malicious computer program that makes illegal advertisements,
Is a malicious program/content that destroys your computer by sometime advertising things deliberately on your computer for you,
Adware is the program that shows you advertisements when you didn't ask for them in your computer,
Is a computer program with illegal advertisements,
Is a computer program that places advertisements illegally,
It is a program that show illegal advertisements on the internet, it is similar to pop-ups,
Adware is a type of malware that is used to gain personal information like passwords and usernames,
Is a program that ensure that everything is secure or information is secure,
A malware that is designed to advertise products offered by sponsors,
Adware is the process of receiving advertisements illegally, if you click on the advert you could be infecting your computer or cell phone

These results show the evaluation methods that are used to evaluate the proposed cyber security awareness programme.

V. CONCLUSION

Cyber space is a complex environment that can advance individuals' experience of electronic dependent activities, but can also place these individuals and their respective nations in a vulnerable state. Cyber space, cyber awareness and cyber security play an important role in the online experience of individuals, and need to be addressed accordingly. The internet and cyber world is a dangerous place where innocent users can inadvertently fall prey to shrewd cybercriminals. These dangers, combined with a large portion of the South African population that has not had regular and sustained exposure to technology and broadband internet access, expose local communities to cyber threats.

A study done by Albrechtsen and Hovden [2] investigated the success factors of security awareness programs. The finding shows that attendees participating in training sessions have a higher success rate than with other training mechanisms, such as posters and presentations. This research study aims to have a high success rate through the use of a formal and interactive cyber security awareness program, as discussed in this paper.

This project addresses the impact that increased broadband access will have on rural South African communities, and how these communities' understanding and acceptance of the technological advances may affect associated security threats to national security and the average South African citizen. This, combined with the fact that there is a large portion of the South African population that has not had regular and sustained exposure to technology and broadband internet access, exposes local communities to cyber threats.

REFERENCES

[1] Abraham, S. & Chengalur-Smith, I., 2010. An overview of social engineering malware: Trends, tactics, and implications. Technology in Society. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0160791X10000497 [Accessed, April 6 2011].

[2] Albrechtsen, E. & Hovden, J., 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), p.432–445.

[3] Alexa, Alexa the Web Information Company. Alexa the Web Information Company. Available at: http://www.alexa.com/ [Accessed April 8, 2011].

[4] Annual Worldwide Damages from Malware Exceed $13 Billion, 2007. Available at: http://www.computereconomics.com/article.cfm?id=1225 [Accessed, April 6 2011].

[5] Baltazar, J., Costoya, J. & Flores, R., 2009. The Real Face ofKOOBFACE: TheLargest Web 2.0Botnet Explained, Trend Micro. Available at: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf [Accessed, April 7 2011].

[6] Caslon Analytics note: Communication statistics. 2005. Available at: http://www.caslon.com.au/statsnote7.htm [Accessed, April 19 2011].

[7] Cnet, 2011. The dangers of remote PC access. Available at: http://reviews.cnet.com/4520-3513_7-5053016-1.html [Accessed, April 19 2011].

[8] Grandjean, E., 2008. A Prime Target for Social Engineering Malware. McAfee Security Journal, 2008(Fall), pp.16-21.

[9] Grobler, M., Jansen van Vuuren, J. & Zaaiman, J., 2011. Evaluating Cyber Security Awareness in South Africa. In Press: ECIW conference July 2011.

[10] IOLScitech 2011. Top five cyberthreats facing consumers. Available at:http://www.iol.co.za/scitech/technology/security/top-five-cyberthreats-facing-consumers-1.1009335 [Accessed, April 20 2011].

[11] Kabilan, M.K., Ahmad, N. & Abidin, M.J.Z., 2010. Facebook: An online environment for learning of English in institutions of higher education? Internet and Higher Education, 13(2010):179-187.

[12] Key Malware Threats: A Brief history, 2009. Available at: http://knol.google.com/k/jj/key-malware-threats-a-brief-history/1mq1t4zz605lf/5# [Accessed, April 6 2011].

[13] Kim, W., Jeong, O.R., Kim. C. & So, J., The dark side of the Internet: Attacks, costs and responses. Information Systems, In Press, Corrected Proof. Available at: http://www.sciencedirect.com/science/article/B6V0G-51J9DS4-1/2/1a75ce9706b13898decd576f47395638 [Accessed, April 6 2011].

[14] Kujawski, M. 2009. Latest mobile phone statistics from Africa and what this means… Available at: http://www.mikekujawski.ca/2009/03/16/latest-mobile-phone-statistics-from-africa-and-what-this-means/ [Accessed, April 19 2011].

[15] Mayer-Schonberger, V., 1998. The internet and privacy legislation: Cookies for a treat? Computer Law & Security Report, 14(3), pp.166-174.

[16] Muralidharan, S., 2011. Hope for Haiti: An analysis of Facebook and Twitter usage during the earthquake relief efforts. Public Relations Review, 37(2), pp.175-177.

[17] Noreen, S., Murtaza, S., Shafiq, M.Z. & Farooq, M., Evolvable malware, Proceedings of the 11th Annual conference on Genetic and evolutionary computation (GECCO '09), 2009.

[18] Ryan, T. & Xenos, S., 2011. Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage. Computers in Human Behavior. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0747563211000379 [Accessed, April 8 2011].

[19] Swartz, M.K., September. Cyberbullying: An Extension of the Schoolyard. Journal of Pediatric Health Care, 23(5), pp.281-282.

[20] TimeLIVE, 2010.Virus breaches 75 000 computers. Available at: http://www.timeslive.co.za/scitech/article314541.ece/Virus-breaches-75-000-computers [Accessed, April 20 2011].

[21] Timm, C. & Perez, R., 2010. Seven Deadliest Social Network Attacks, Syngress. Available at: http://www.amazon.com/Seven-Deadliest-Social-Network-Attacks/dp/159749545X/ref=sr_1_1?ie=UTF8&s=books&qid=1303301377&sr=1-1.

[22] VideoSwiper, 2011. Video Script Review – Social Media. Available at: http://www.videoswiper.com/review-socialmedia.html [Accessed, April 19 2011].