International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:11, 2013

Engagement of Young People in Social Networks: Awareness and Security

Lynette Drevin, Günther R. Drevin

***Abstract*—**Numerous threats have been identified when using social networks. The question is whether young people are aware of these negative impacts of online and mobile technologies. Will they identify threats when needed? Will they know where to get help? Students and school children were part of a survey where their behavior and use of Facebook and an instant messaging application - MXit were studied. This paper presents some of the results. It can be concluded that awareness on security and privacy issues should be raised. The benefit of doing such a survey is that it may help to direct educational efforts from a young age. In this way children – with their parents – can strive towards more secure behavior. Educators can focus their lessons towards the areas that need attention resulting in safer cyber interaction and ultimately more responsible online use.

***Keywords*—**Facebook, Instant messaging, MXit, Privacy, Social networks Information Security awareness education, Trust.

I. Introduction

THE way people interact with each other online has changed a lot since the development and use of personal computers, the Internet and, more recently, mobile devices. Our social relationships are being changed by ICT (Information and Communication Technologies) in ways that we cannot comprehend. Poullet [1] refers to the different contexts that ICT let us express ourselves and where more personal services are available. Social networking applications are technologies that let boundaries disappear and let people interact in new ways. Applications such as Facebook and other online chat programs are favorite pastime activities for people – especially young adults and teenagers.

The focus of this paper is to discuss a survey done among young people to understand their use and perceptions of social networks such as Facebook and MXit [2]. Security awareness issues will be looked into in order to assess which education topics have to be considered in awareness programs. Facebook is a social network founded in 2004, originally among Harvard University students but it also became very popular at other colleges and then it propagated to school children and around 2006 it was open to the world. According to Langheinrich & Karjoth [3] the user base of Facebook was around 125 million users in 2010. Another very popular networking application in South Africa is MXit. MXit is a free online mobile chat application where the user can play, shop and "explore a multi-million user social network", [4]. MXit can be enabled on old and new phones and according to the MXit website "your old phone can be made smarter". However, many security and privacy risks have been identified with the use of these social networks. Previous studies accentuated schoolchildren's use of the Internet and the threats that go hand in hand with this [5]. A high level of unsafe Internet behavior was reported such as chat activities with unknown persons, sharing personal information with strangers and personal meetings with these unknown persons.

In order to assess these risks it was decided to do a study in our community to ascertain how the young people behave when using two of these social network sites namely Facebook and MXit. A questionnaire was used to gather information on their use thereof and their security perceptions of these sites. Secondary school pupils as well as university students were part of the study. This paper will discuss some results of the survey.

The rest of the paper is structured as follows. Section II will elaborate on the security issues involving the use of social networks. Section III will describe the survey done among young people. Section IV will give details on the results of the questionnaire and Section V will conclude the paper.

II. Using Social Network Sites

According to Valcke et al. [5] the introduction of computers at school and at home and subsequently the use of the Internet have raised many security issues such as safety, privacy and abuse. It is even more so with the evolution of social networks. The question that comes to mind is whether young people (and others) are aware of the accompanying dangers and how they will handle it. Langheinrich & Karjoth [3] referred to the risks that companies and institutions face and have to combat when social networks are visited and used by employees. Not only are there lots of opportunities with these technologies, for example knowledge transfer, but the challenges also accumulate. A company's image can be impacted negatively; information can get in the wrong hands etc.

Rosenblum [6] studied various privacy risks of social network sites and the following are some of the issues that emerged from his study.

- Privacy redefined: Some people have the perception that their communication is private online.
- The boundary between public and private: The way that people are willing to disclose personal information has changed over time, some people need to tell everybody what they think or do during each day. A world without

L. Drevin is with the North-West University (Potchefstroom Campus), Computer Science & Information Systems, South Africa (phone: +27 18 2992534; e-mail: lynette.drevin@nwu.ac.za).

G.R. Drevin is with the North-West University (Potchefstroom Campus), Computer Science & Information Systems, South Africa (phone: +27 18 2994265; e-mail: Gunther.drevin@nwu.ac.za).

Facebook is incomprehensible to them.

- Security and privacy risks: Internal risks such as communication on the Internet emerge. It is recorded and stored, permanently and it can be disseminated very broadly. External risks can be unauthorized use of information by third parties.
- Social predators: Sexual offenders have already exploited the social network sites and minors have been approached by stalkers and child molesters.

Security risks such as malware can be introduced in an organization or on home users' computers via social online sites unknowingly by unaware computer users. Examples of such malware are [7]:

- Koobface – a worm that targets Facebook to collect information of users
- Boonana – a malicious program written in Java targeting Mac platforms
- Bugat - Collecting information in a key logging way

Even though there are numerous risks involved in the use of social media there are important benefits for the home user and corporate environment and therefore we cannot ignore these risks.

Young people especially are vulnerable and may become a target due to their immaturity. The legal system must also be extended to include the protection of minors and their privacy in cyberspace [1]. Privacy is of great concern when social network sites are used. Facebook and other interactional applications have become a preferred way of communication. These sites are relatively easy to use and personal and other information that are uploaded can easily be reviewed – also by unrelated parties. A solution that is proposed by Rosenblum [6] is that users must use common sense and review what they post and review what is available about them. One must be careful about what is morphed from your personal live into the cyber world, which may exist digitally forever. Although solutions are proposed for these challenges we need to determine how our young people use the social networks. The next section discusses the survey that was done among young people, regarding their use of social networks online as well as on mobile phones

III. Discussion of Survey

This project used a questionnaire that was developed to get information on the use of Facebook and MXit by young people. The questionnaire consisted of five sections.

Personal, Facebook, MXit, computer use and knowledge and ethics questions were included in the questionnaire. This was handed to the respondents on paper for completion.

This paper focuses only on a subsection of the questions relating to social network behavior and views on security. These will be compared between different age groups. The school pupils consisted of three groups namely grade 8, grade 10 and grade 11. The student groups consisted of a second year IT group, a mixed group of students who were approached via electronic questionnaires and an honors group of IT students. A total of 61 school learners and 80 students participated in this survey.

The next section will discuss some of the results of the questionnaire.

IV. Results

Some of the background information of the respondents is as follows. The number of females decreased in the older age groups. The school pupils' ages varies from 14 - 19 years (grade 8 to 11) and the students' ages are in the range of 19 - 24 years. Most of the school learners stay at their parents' home and the students live in hostels or privately rented room and a smaller portion are still studying from home.

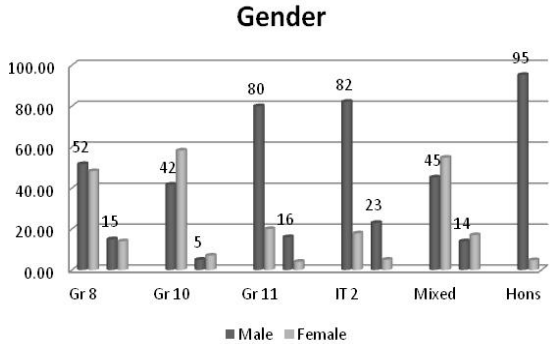

Fig. 1 Gender of respondents

More male than female students took part in the survey. This reflects the fact that more males were enrolled for IT than females. It seems that female IT school learners dropped out of IT as subject as they progress to later grades.

The following figures show some of the information on the use of Facebook. Most of the respondents are Facebook members or are planning to become members.

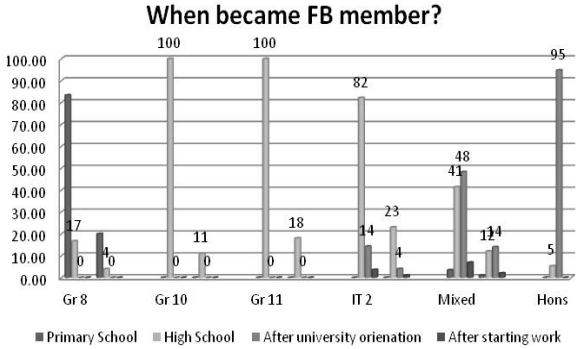

Fig. 2 Stage of life when becoming a Facebook member

It can be seen that the younger groups of respondents started using Facebook at a younger age than the older groups.

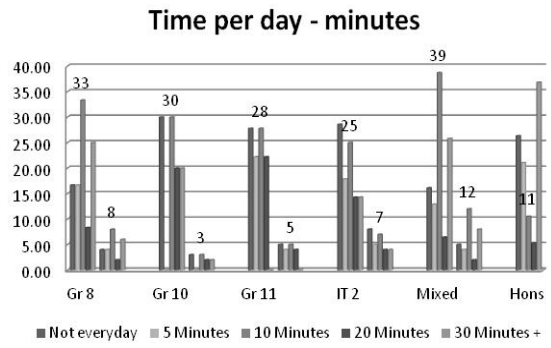

Fig. 3 Time that is spent on Facebook

Fig. 3 shows that the older respondents (students) spend more time on Facebook than the school learners.

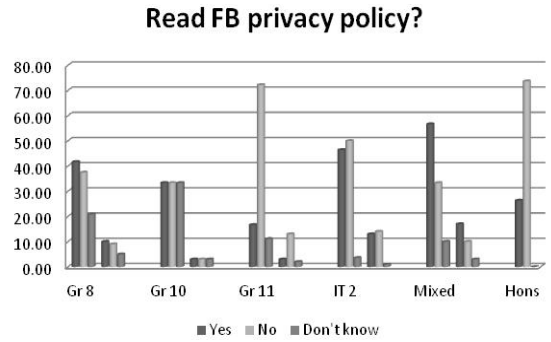

Fig. 4 How many respondents read the Facebook policy?

Fig. 4 indicates the number of respondents that read the policy of Facebook. The school children are unsure about the privacy policy of Facebook, which may show towards unawareness. This then has to be an indication for awareness programs.

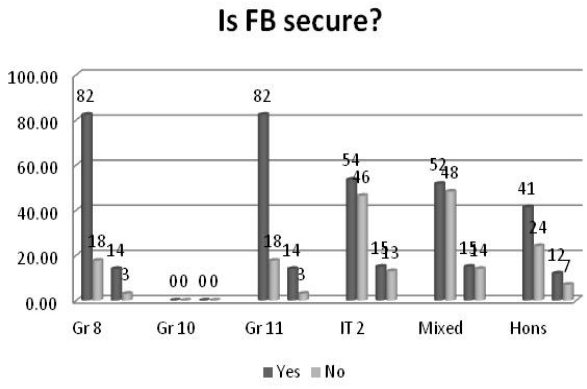

Fig. 5 Number of respondents that feel that the use of Facebook is secure

Fig. 5 indicates that more school learners than students think that FB is secure. This might indicate their naivety to trust easily. This must also be addressed in educational efforts.

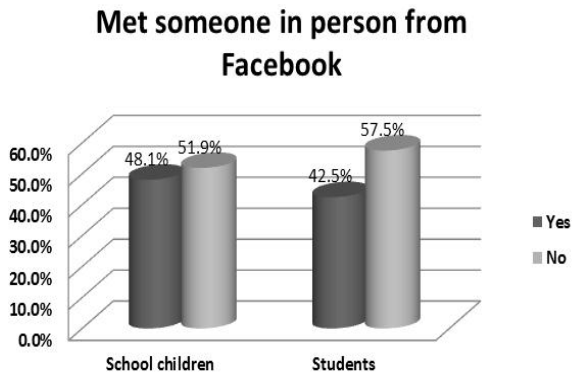

Fig. 6 Number of respondents that met Facebook "friends"

It can be seen from Fig. 6 that 48% of schoolchildren met someone new from Facebook. 42% of students met someone in person from Facebook. It is seen that young people often meet up with complete strangers – they trust easily.

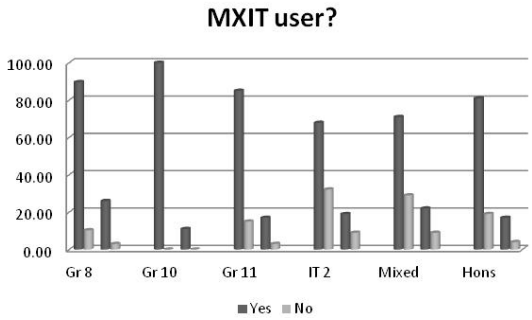

Fig. 7 Number of MXit users

Fig. 7 indicates that most of the respondents are registered users of MXit. MXit allows users to change their profiles, has status updates and have chat rooms where one can meet new people and socialize in a virtual way.

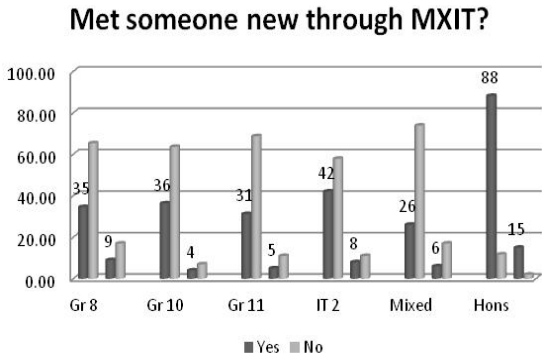

Fig. 8 Numbers of MXit users that met new persons through this platform

Every group of respondents met someone new through MXit – as it was with Facebook environment. Again this shows the ease of trust and perhaps naivety of young people.

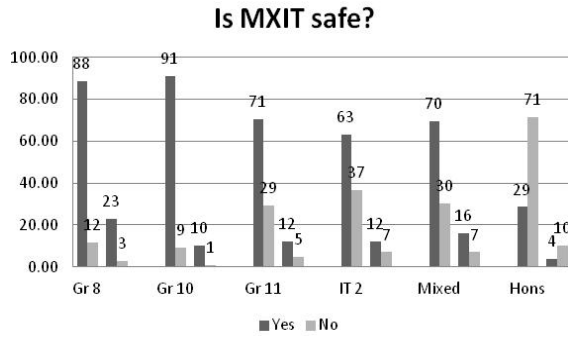

Fig. 9 Numbers of respondents that feel the use of MXit is safe

Fig. 9 indicates that more students than schoolchildren think that MXit is not safe – it could be that schoolchildren trust easily or are unaware of dangers. MXit has a link to pages for online safety but these are rarely read before the use of this instant messaging service.

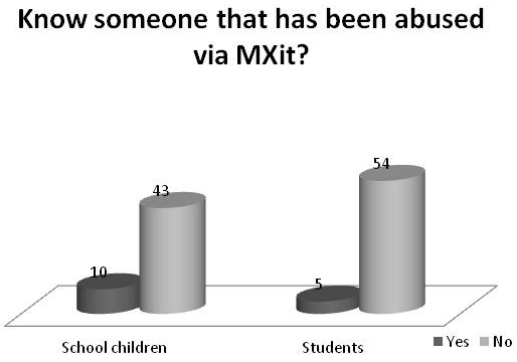

Fig. 10 Number of respondents that know an abused victim

Fig. 10 indicates that - although not high in numbers - it is alarming to see that there are schoolchildren and students who know someone that has been abused via MXit. Ease of trust must be a key point to address in awareness programs.

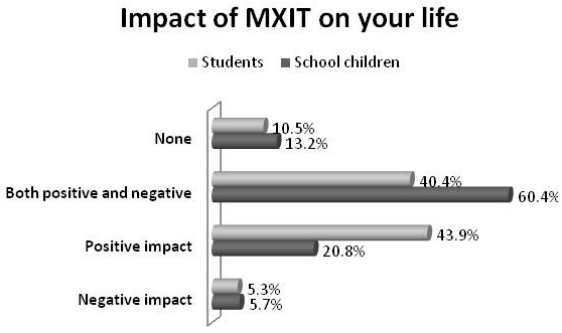

Fig. 11 Perception on MXit's influence on life

Fig. 11 indicates that the youth feel differently on the impact of MXit on their lives. Both positives and negative impacts have been reported.

The following questions are knowledge or behavior type of questions regarding safe online behavior.

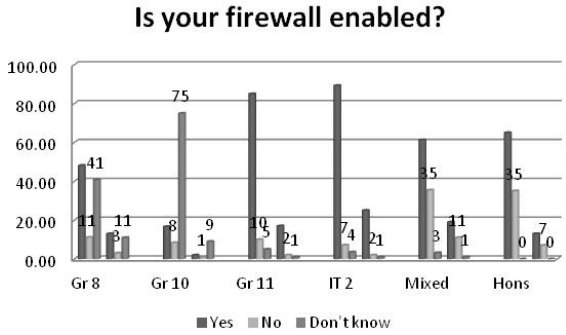

Fig. 12 Number of young ones that enabled their devices' firewall

The question was stated if their computer's firewall is enabled. There are more 'I don't know' answers from the school learners than from the students, which may indicate unawareness of the technology in question. Fig. 12 again shows that training can play a role in helping youngster to become more knowledgeable regarding secure online actions.

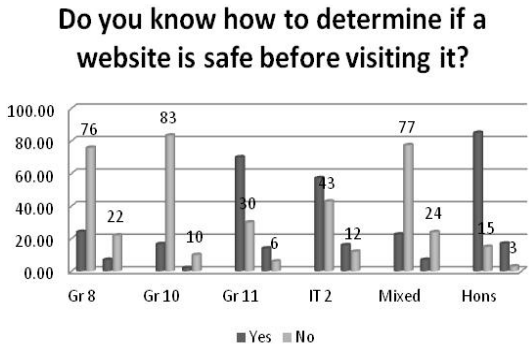

Fig. 13 Number of respondents that have knowledge of safe websites

The question was asked whether they know how to determine if a website is safe to use. Fig. 13 indicates that the group of honors students is the most aware of how to answer this scenario. Younger school children are the most vulnerable groups.

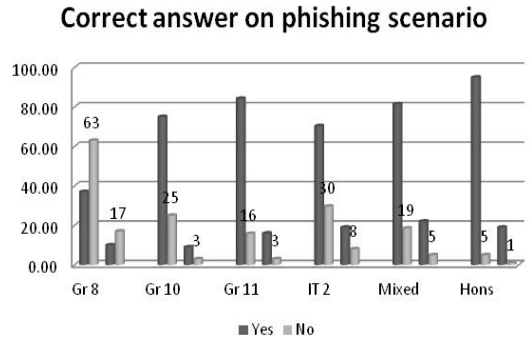

Fig. 14 Knowledge and behavior on phishing

A scenario was put forth to the respondents for them indicate what they would do in a phishing attack. Fig. 14 indicates that the school children should be made more aware

of phishing incidents as they could not answer the question correct. They may unknowingly give personal information away because they do not recognize a phishing attack.

Fig. 15 Give away passwords

The question was asked whether they would be prepared to give away passwords. Fig. 15 shows the number of respondents that are prepared to share password with other people. In this regard, they should be made aware of password management in order to keep their personal passwords safe.

Fig. 16 Use of employer's IT facilities

Fig. 16 indicates responses to a question regarding their future behavior. It was asked if they would use their employer's computers for own gain. It shows the number of young people that feels it would be acceptable to use employers' computer facilities to do their own work. This refers to and ethical situation and as such indicates that ethical dilemmas should also be included in educational programs.

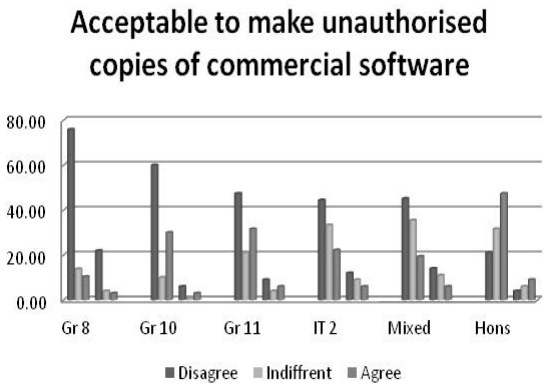

Fig. 17 Unauthorized copying

A question was asked whether they think it is acceptable to make unauthorized copies of commercial software. Fig. 17 shows that younger children feel that illegal copying of software in not acceptable whilst older students do not feel as strong. Again this shows that ethical issues as well as legal matters need attention in education.

The above discussions present some of the findings of this survey. Although the number of respondents is low and the results are not generalizable this type of survey still indicates the problem areas that should get attention. According to Pfleeger & Pfleeger [8] information security consist of different aspects including technology and social issues. The above findings show that young people should be educated and be made aware in both these areas. Their behavior and knowledge regarding their IT devices and their attitudes should be made more security alert.

V. Conclusions and Future Considerations

Security awareness is important when social networks are used. This paper focused on some responses of young people regarding their use of Facebook and MXit and their engagement with social media platforms.

It could be seen from the data above that a need exists to make the youth more aware of their safety and encourage them to behave in a secure way. Some guidelines could include aspects such as respecting your own and others' privacy, not meeting strangers from these sites, change privacy settings to be more limiting, etc. General knowledge on aspects such as firewalls use, phishing, viruses and how to update security controls must be included in awareness campaigns run by school administrators, parents and lecturers. The benefit of a survey such as this is to identify and determine key areas of concern and to address these in awareness efforts. This may lead to more responsible behavior from the future employees as well as decreasing the risks generated by people using/misusing social networks.

Future work includes aligning information security educational efforts with the results and outcomes of these types of surveys.

REFERENCES

[1] Y. Poullet, "e-Youth before its judges, Legal protection of minors in Cyberspace," in *Computer Law & Security Review* 27, 6-20, 2011.
[2] L. Drevin, L & G.R. Drevin, "Young People: How safe are they when using social networks," Extended abstract. in *Proc. of the 7th World conference on Information Security education*, Lucern, Switzerland, 2011.
[3] M. Langheinrich, & G. Karjoth, "Social networking and the risk to companies and institutions," *Information Security Technical Report* 15, 51-56, 2010.
[4] MXit. http://www.mxitlifestyle.com/ Online: Date of access 21 Aug 2013.
[5] M. Valcke, T. Schellens, H. Van Keer, & M. Gerarts, "Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study," *Computers in Human Behavior* 23, 2838–2850, 2007.
[6] D. Rosenblum, "What anyone can know, the privacy risks of social networking sites," *IEEE Security & Privacy*, May-June, 40-49, 2007.
[7] Osterman Research, Inc. "The risks of social media and what can be done to manage them", 2011.
[8] C. Pfleeger & S. Pfleeger, *Security in Computing.* Upper Saddle River, NJ.: Prentice Hall, 2007.