2016

An investigation into the security behaviour of tertiary students regarding mobile device security

Martin Park
North-West University, Potchefstroom, martinpark02@gmail.com

Lynette Drevin
North-West University, Potchefstroom, lynette.drevin@nwu.ac.za

14. An investigation into the security behaviour of tertiary students regarding mobile device security

Martin Park
North-West University, Potchefstroom
martinpark02@gmail.com

Lynette Drevin
North-West University, Potchefstroom
Lynette.Drevin@nwu.ac.za

Abstract

The use of mobile devices is becoming more popular by the day. With all the different features that the smart mobile devices possess, it is starting to replace personal computers both for personal use and business use. There are also more attacks concerning security on mobile devices because of their increased usage and the security measures not as effective and well-known as on personal computers. The perceived perception is that the young adult population does not act safely and they have a low level of technical advanced knowledge when using their mobile devices. Mobile users are largely responsible to protect themselves and other users from a security viewpoint. This paper reports on a study including a survey done regarding the behaviour of tertiary students concerning security of their mobile devices. Aspects of mobile device security will be discussed and the current status of tertiary students' behaviour regarding mobile device security will be presented resulting from a survey conducted at a South African University. Findings indicate that tertiary students have diverse behaviour levels concerning mobile device security. The value of these results is that we can focus on specific content when educating smart device users on the subject of security including avoidance of risky or unsafe behaviour. Recommendations in this regard are presented in this paper.

Keywords

Mobile Device Security, Behaviour, Awareness, Smartphones, and Tertiary Students

1. Introduction

Mobile device security has become an increasing problem in the modern day user's life. If a mobile device is not used in a secure manner it can lead to various negative security implications such as the leaking of sensitive information and virus infections. Therefore it is important that users are aware of mobile device security and that they act securely.

In recent years Personal Computers (PC) has been a more attractive target for cyber attackers than mobile phones. There were fewer ways for hackers to attack the mobile phones because of the lack of technical sophistication of mobile devices regarding security. Even though mobile devices are not as powerful as some PCs, the devices have numerous features and are definitely assets worthy of protection. Because mobile devices are not as powerful as computers they are more vulnerable to different threats (Botha *et al.* 2009). This is however changing as we acknowledge the sophistication of new smart mobile devices. The broad definition of mobile devices includes laptops, but this discussion's focus is limited to smartphones and tablets. These are the devices which are almost instantly accessible to most

users as the carry it easily with them. Androulidakis and Papapetros (2008) state that mobile devices are no longer used only for voice transmission. Mobile networks along with the devices are now also used for business and financial transactions and exchanging data and information. According to Lawton (2008) smartphones are getting less expensive and this allows more people to use smartphones. These mobile devices run on sophisticated operating systems, have short range Bluetooth radios, and have access to the Internet, email, instant messaging and multimedia messages. All of these different features allow attackers to install malware on the smartphones or some users run the malware inadvertently on their devices. Because of modern developments in the industry, observers have to pay more attention to mobile malware as mobile devices become a bigger threat to its users (Lawton, 2008; Allam *et al. 2014)*. Malware is not the only threat towards mobile devices. Other techniques such as phishing, social engineering and direct hacker attacks have already found their way to attack mobile devices (Landman 2010). Another reason for more attacks on mobile devices is the tremendous increase in usage of these devices. This is supported by Flurry Analytics, a research firm that states that the adoption of smartphone devices are ten times faster than the adoption of PCs in the 1980s, double the time of the Internet boom in the 1990s and three times faster than social media adoption (Heinrichs & Jones 2013).

The study of Androulidakis and Papapetros (2008) show that tertiary students do not always have a feeling of safety and they lack technical advanced knowledge when using their mobile devices. Security and privacy issues have a big effect on mobile users. They are largely responsible to protect themselves and protect other users in this mobile domain. Robinson (2014) states that according to a survey done by Enterprise Management Associates (EMA) only 56 percent of corporate employees were involved in any form of awareness training. In a book "Cybersecurity: the essential body of knowledge", Shoemaker and Conklin (2012) include IT security and awareness as a crucial element within organizations to ensure secure behaviour - indicating the significance of awareness.

The ways that people work are changing due to business mobility (Harris & Patten 2014). In the business world today organizations are increasingly depending on smartphones to do different business tasks. The tasks are creating more opportunities for smartphones to be attacked and mobile devices are attractive targets for criminals. There are organizations that have not yet implemented adequate security controls and policies to guide users with the use of smartphones (Landman 2010). Businesses are indeed becoming more aware that they need to have a mobile security strategy in place and this is then a problem they need to address (Harris & Patten 2014). With the rapid increase of mobile workers and people relying on their mobile devices to complete their work, the threats towards smartphones are increasing (Landman 2010). A big danger is however when the user mix personal and business activities. The problem is that the user must then distinguish between different uses and the corresponding security rules that apply to each activity. Users lack awareness of the threats and potential damage the attack can cause on the smartphones to them and to the organization (Landman 2010).

From the above discussion it is seen that in the future mobile phones may be used instead of PCs either for personal use or business use. The problem is that the users are not fully aware that the smartphones need the same level of security and protection than computers (Lawton 2008). According to Benenson *et al.* (2012) an interesting question that is still unanswered is whether the users see the similarity between their smartphones and the PCs. The functionality and the threats are very similar for both kinds of devices, but the users' perceptions and attitudes may differ. This paper focuses on the security awareness of tertiary students

regarding mobile devices seeing they are the workforce of the future (Park 2014). The aim of the paper is to describe the following: What is the behaviour of tertiary students regarding mobile device security and what can we learn from this? Awareness is often defined in terms of behaviour, knowledge and perception. In this study the main focus will be on behaviour, although some aspects of knowledge and perception will also be referred to. The rest of the paper is organized as follows. Section 2 focuses on PC and mobile device security, mobile malware and users' awareness of mobile device security. Section 3 presents the methodology followed in this study. Section 4 presents the data collected, data analysis and results of the survey. Section 5 discusses the limitations to the study and possible future work. Section 6 presents the recommendations and conclusions.

2. Background

A literature review was done on search terms such as comparing PC security to mobile security, mobile malware and user awareness of mobile device security. Each of these topics is discussed in this section.

2.1 PC security vs mobile device security

In the new era of mobile devices better known as smartphones today, the capabilities of the mobile devices can be compared to those of PCs. In addition to these capabilities mobile devices also offer a big selection of connectivity options such as GPRS (General Packet Radio Service), GSM (Global System for Mobile communications), HSPA (High Speed Packet Access), UMTS (Universal Mobile Telecommunications System), Bluetooth and IEEE 802.11. It is speculated that malware for mobile devices will start to follow a similar trend as malware for PCs where the number of malware for mobile devices will increase significantly. Another reason why mobile devices will become a bigger target for attackers is because users are increasingly starting to use mobile devices for sensitive transactions such as online banking and online shopping (Ott 2014). Security of mobile devices is important when considering that these devices can store and access similar data and services as computers. Therefore there is a need for similar security provisions for mobile devices as for computers.

Research done on security and privacy perceptions regarding Android mobile devices shows that users are not very keen to use their mobile devices for money related tasks (such as online banking and shopping) or for sensitive data (such as health records and social security numbers). They prefer to rather do these kinds of tasks on their PCs (Ott 2014). Mobile devices can accommodate almost as much data, services and applications as PCs despite the difference in size of these devices.

2.2 Mobile malware

There is a large amount of malware types that use various ways to propagate and infect devices of victims (Peng *et al*. 2014). La Polla *et al*. (2013) argue that malware is any kind of software or program code that can be annoying, intrusive or hostile. Mobile malware can spread through different vectors such as a link to a site where the malicious code can be downloaded included in a SMS, infected attachments included in a MMS, sending infected programs via Bluetooth and downloading applications that contain a form of malware. When malware targets mobile devices the main goals of the malware is to gain access to personal data stored on the device and the credit of the user. Malware is grouped into the following most common categories according to its features (Peng *et al*. 2014; La Polla *et al*. 2013): Viruses and Worms, Trojans, Rootkits, Botnets, Spyware.

Becher *et al*. (2011) mention that there are several possible attack strategies and forms of malware behaviour. Firstly there is information or identity theft. An example of this is when a mobile game is downloaded from a third party application store and the game is able to track the location of the users. A detailed profile of the victim can be collected because the mobile device is carried by the user everywhere he goes and a variety of information types such as GPS coordinates, credentials, contacts, corporate and private documents and various forms of communications (SMS, MMS, email etc.) can be obtained. Secondly there is eavesdropping. Different routines are used to capture voice calls and to record any conversations silently which are in range of the built-in microphone. Mobile botnets are also an attack strategy. These infected mobile devices are the perfect remote controlled "machines" attackers are looking for. Along with mobile botnets Denial of Service (DoS) attacks can be launched against the mobile devices. One technique that can be used is to drain the battery of the device by launching an attack that use a large power consumption such as having malware that use all the available CPU cycles for junk calculations. The service of the mobile device can also be disabled by deleting or corrupting the essential data stored at difficult to reach locations. Lastly the attacks can also be focused on the economic loss. It can either be by creating chaos between the service provider and the mobile device user or by getting access to private financial information stored on the device and do transactions on behave of the user without the awareness of the user.

Peng *et al*. (2014) noted that there has been an increase of malware over the years for various reasons including decrease in price of mobile devices, open source kernel policy, storage of private data on mobile devices, increase in capability of mobile OS, etc. The awareness of users regarding the use mobile devices and security is therefore important and the next section presents this topic.

2.3 Users' awareness of mobile device security

Awareness of mobile device security can be described as the knowledge, attitude and behaviour that users apply to the security when using their mobile devices (Allam *et al*. 2014). Security awareness programmes are implemented to raise the awareness level of users to a specific risk area. According to Kruger and Kearney (2006) there are three factors/elements which should result when the awareness levels are addressed namely:

- Knowledge: what the users know;
- Attitude: what the users think;
- Behaviour: what the users do.

These factors are addressed in awareness programmes in expectation that the security risk will be reduced. The aim of training and improving of awareness in organizations is to ensure a reliable level of secure practice (Shoemaker & Conklin 2012). These awareness initiatives should also shift the focus towards mobile device use to keep up with the growth in this technology. Harris *et al*. (2014) mention that there is a variety of weaknesses in the attitude and behaviour regarding security of mobile device users. Most people have the attitude that security problems faced in the past will be diminish when a more technology literate user becomes the norm. Results from their survey also support this. In a study done by Jones *et al*. (2014) almost half of the student respondents did not concur that using a password was important, less than one third of the students do not log out of their emails and social networking when not in use, half of them did not hesitate to open an attachment from an unknown source and 40% limit their Wi-Fi activity to protected networks.

According to a study done by Ophoff and Robinson (2014) almost all of the respondents who use IOS and Symbian, trust the app repositories. In a study done by Mylonas *et al*. (2013) it is found that most users believe that apps that are downloaded from different app repositories are secure. It is seen that this assumption is incorrect according to Mylonas *et al*. (2011) where it is stated that the security controls used by app repositories are not used in all of them. Anderson *et al*. (2010) also support this by stating that all malicious applications cannot be filtered by application testing. Users are also not aware of the application testing to test against malicious behaviour that occurs in the app repositories. In Ophoff and Robinson (2014) it is mentioned that two thirds of the respondents are not aware whether or not the apps in the repositories have been through security testing. In Mylonas *et al*. (2013) it is indicated that the users trust the app repositories even though they are not sure whether app testing occurs or not. Repetitive warning messages are ignored by users when downloading or using apps. According to Bőhme and Kőpsell (2010) less attention is paid to consequent warning messages by users when the warnings resemble an End-User License Agreement (EULA). Al-Hadadi *et al*. (2013) found that more than half of the respondents in the study did not know how to follow safe usage instructions and they were not aware of the problems regarding mobile device security and best practices for security.

The findings in the study of Mylonas *et al*. (2013) suggest there is a poor adoption of security controls by mobile device users. These security controls include physical controls such as device password, lock and third party security controls software such as anti-viruses. The adoption rate of physical controls is poor. Most users use a device password lock but controls such as encryption, remote data wipe and remote device locator are not regularly used. Users feel that the security software on mobile devices is not essential. This feeling can be based on the drainage of the battery by the software and slowing down the performance of the mobile devices. When looking at third party security software, it is seen that more users install this type of software on their PCs but not on their mobile devices. This indicates that the users are not aware that security threats on mobile devices are as dangerous as on PCs. Similar results are shown in the study done by Ophoff (2014). Only 27% of the respondents use mobile device security software compared to 97% who use PC security software. The study also showed that only half of the users who believe that security software are essential are in fact using security software on their devices.

Ophoff (2014) compared his findings with those of Mylonas *et al*. (2013) and the following findings stood out:

- Users can be left vulnerable because they trust app repositories and believe that the repositories are secure.
- Users who believe they are experts on an IT level and those who have undergone information security courses have a more deterministic view on application testing and this affect their level of trust on the app repositories.
- Not much attention is paid to privacy and security when applications are installed on mobile devices by users, although some users are aware of malicious applications.

The above literature reviews indicated different threats regarding mobile and wireless communication technologies as well as previous studies focusing on the awareness of users regarding mobile device security. The next section will present the methodology used for this study and the development of the measuring instrument.

3. Methodology

The philosophical paradigm of positivism, which underlines the scientific method according to Oates (2006) was mainly followed in this study as data was most statistically analysed. A survey was done to gather users' data making use of an online questionnaire. Participation was voluntarily and anonymous. Different factors/elements that are important to assess users' awareness of mobile security were investigated in existing literature and were used to construct the questions. Due to space restrictions the questionnaire is not listed in this paper. Qualitative data was also collected and this was analysed in an interpretative way.

This questionnaire was designed to mainly assess tertiary students' behaviour, but also knowledge and attitude or perception regarding mobile device security. Behaviour is seen as "a function of the interaction between the person and the environment" (Kassin *et al*. 2008). In the case of mobile device security it can be assumed that behaviour indicates a mobile device user how he/she interacts with technology. Our attitudes influence our behaviour through our conscious decision making – this is according to the theory of planned behaviour (Kassin *et al*. 2008). (There are also other determinants that influence our behaviour – e.g. subjective norms. This is however not in the scope of this paper to discuss it further). The last aspect that influences awareness of users according the Kruger and Kearney (2006) is their knowledge. Are users familiar with security terms and do they know what it means? These aspects were then included when the questionnaire was developed to assess the awareness levels of young users. First some biographical questions were asked to get a better background of the respondents. Secondly, questions regarding behaviour, knowledge and attitude of mobile device security were asked. Lastly there was an open ended question asking for comments from the respondents.

This section presents the data collection process. The questionnaire was developed in Google Forms. An email was sent out to participants with a link to the online questionnaire. Before the questionnaire went live a pre-test was done to make sure that the questions were understandable and clear and that the process works smoothly. The target group of the study was tertiary students attending a South African university. They will be in the workplace within the next few years. Emails were sent out to under- and post graduates including students from all of the faculties at the university. There were 217 responses that could be used in this study. Statistical analysis was done on the data obtained from the respondents to assess what tertiary students' awareness levels are regarding mobile device security.

To get a measure of internal consistency of the questionnaire, the Cronbach alpha coefficient was calculated. The Cronbach alpha coefficient for the questionnaire regarding behaviour was 0.628 and for the questionnaire regarding attitude and opinion was 0.763. Kilne (2000) states that a value of 0.8 is generally accepted for cognitive tests. A suitable cut-off point for ability tests is 0.7. A value below 0.7 can realistically be expected when dealing with psychological constructs because a diversity of constructs is being measured (Field 2009).

The next section presents the results and interpretation of the data of this survey.

4. Survey results

4.1 Results from descriptive statistics

The survey was done among a diverse of tertiary students at a South-African university. Table 1 indicates the demographic information of the respondents. Respondents are mainly part of the white ethnic group and most of them have Afrikaans as their home language. This

is as a result of the feeding area of the university having more white, Afrikaans speaking students.

	Response	Frequency	%
Year of study	1st	24	11.%
	2nd	91	42%
	3rd	42	19%
	4th or more	60	28%
Level of qualification	Under graduate	176	81%
	Post graduate	41	19%
Gender	Male	132	61%
	Female	85	39%

Table 1: Respondents demographics

An answer to the question of how long they have been using a smartphone the results indicate that the respondents in the study are very familiar with smartphones as 87% of them indicated that they have been using a smartphone for longer than 5 years up to the time of the survey. Android is the most popular operating system (OS) on smartphones used by the participants in the study. The second highest OS that is used is IOS. Fig. 1 indicates the use of the different smartphone operating systems.

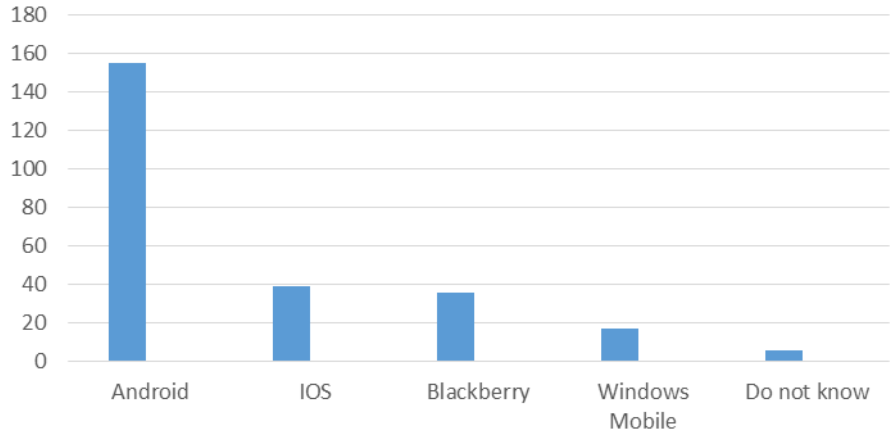

Figure 1: Different operating systems used

Regarding the level of IT expertise the following was seen in the study. 45% of the participants felt that they have a novice to moderate level of IT expertise, while 55% felt that they had a good to excellent level of IT expertise. Asked if they often install new applications on their mobile devices the results indicate that it is indeed the case. 65% of the participants showed that they often install new applications. The problem relating to security that can be seen when applications are installed is that the users do not read the license agreements when installing the software. When a security message appears while installing or using the application, there is a slight increase of people reading the security message. Fig. 2 shows the comparison of these two aspects.

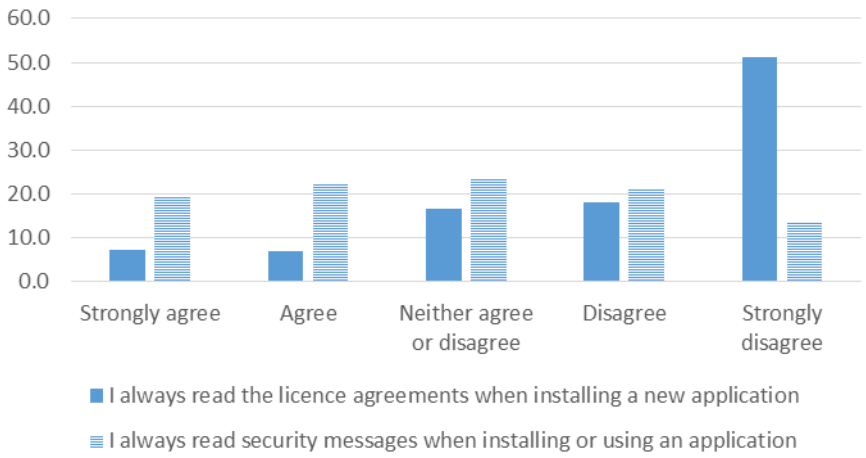

Figure 2: Comparison of reading security messages and license agreements (%)

Personal and business data are both kept on the users' mobile devices. When asked if they store personal and other data on their devices only 27% disagreed that they store personal data on their devices and 43% disagreed that they store business data on their devices. This can be problematic, because when there is an attack on a device both personal and business data can be intercepted and compromised if there are not adequate security measures. Mobile banking has become very popular and easy to use. Along with the mixing of personal and business data storage on the devices, it is perturbing that only 22% of the participants save their banking info encrypted on their mobile device.

When the location services are turned on on the mobile device, there can be a continuous tracking of the location of the user. A user therefore must be careful when enabling his location services. A question relating to the use of location services resulted in the following: From the results it is seen that there are mixed results as 27% indicated that their location services are on all of the time and 55% said their services are not on all the time.

Protecting a device with security software is a vital component nowadays. All devices need to be protected. When the users were asked about protection of their mobile devices in terms of security the results were as follows: It seems that some users think that only their PCs need protection. In fig. 3 it can be seen that 185 participants stated that their PCs are protected while 143 stated their mobile phones are protected with security software. However only 60 of the participants indicated their tablets are protected.

Protection mechanisms are important for the security of mobile devices. There is a good adoption rate of the most common protection mechanisms used by users as can be seen in fig. 4. One of the protection mechanisms is a lock or PIN. 68% of the respondents use this mechanism when their device is switched on, 51% use it when they want to get out of standby mode on their device and 25% use it to get access so certain apps.

When looking at the attitude of the participants regarding mobile device security it was seen that they are aware of the security threats for mobile devices. 78.3% of them felt that security software is essential for mobile devices and 80% of them believed that security controls must be enabled on mobile devices. This support the fact that they are aware of the different attacks that can be launched on a mobile device.

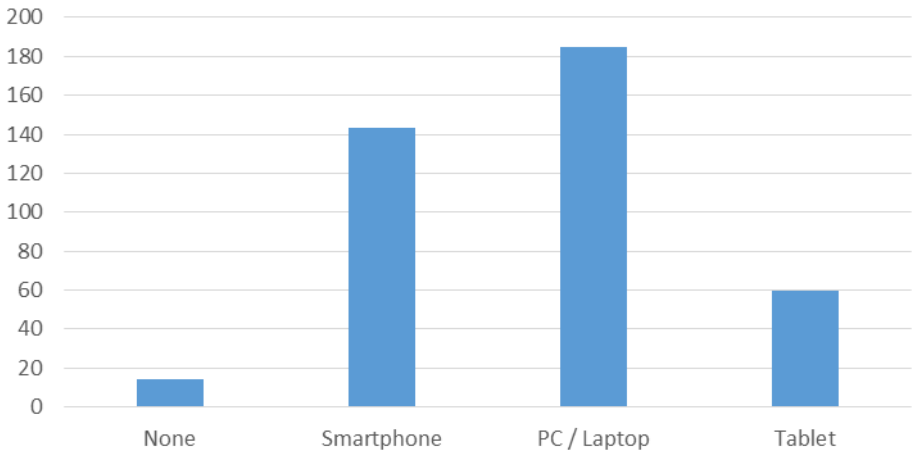

Figure 3: Protection of devices with security software

A good inidcator for users' security awarenes is the knowledge regarding security terminology. Certain questions were asked to assess the users knowledge. 96% of the participants know what an anti-virus program is. This is positive because it is one of the first security mechanisms that has to be be installed on a mobile device to operate securely. A slight worry is that only 54% know what phishing is and only 48% know what a worm is. It is important for users to know about these different attacks. It will make them more aware and then they may operate more securely on their mobile devices. It is a fundametal object for security awareness that users take responsibility for their actions as indicated in a study of Drevin *et al*., (2007).

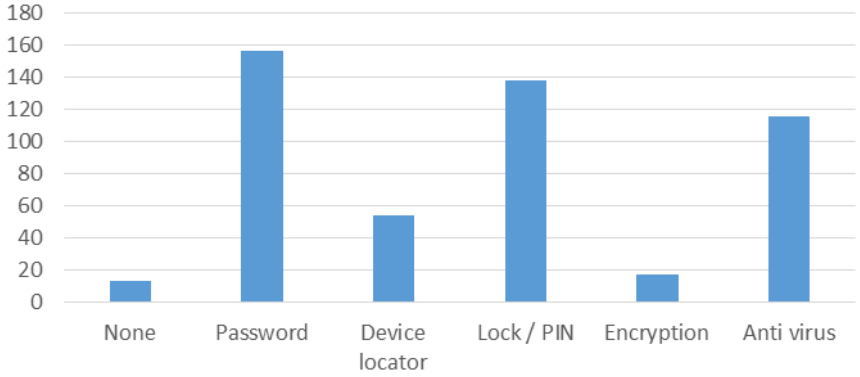

Figure 4: Protection mechanisms used on mobile devices

4.2 Results from interpretive statistics

Different T-tests were carried out to determine differences in gender or level of studies regarding their mobile device security behaviour. The results showed that the mean for male participants were 3.2159 and for female participants 3.2294. There is thus a small difference. Thus males and females did not answer different regarding behaviour. There was a small difference in the mean for the year level namely 3.2209 for under graduate and 3.2226 for post graduate. The Sig value was 0.781 which implied that equal variance was assumed. The reason may be that almost everybody has been using a mobile device for a lengthy period up

to this study as shown in the results where 188 participants have been using mobile devices for 5 years or longer.

5. Limitations and future work

This paper presents a part of the results from the survey conducted to assess security awareness of tertiary students. Only tertiary students were used as participants seeing they are the workforce of tomorrow. A mobile application was developed as a training method for use by tertiary students including relevant topics for improvement of security behaviour. This will be reported on in another research output.

Future work that may follow from this study include:

- Similar studies to include all users.
- Comparative studies between different user groups.
- Developing awareness programs based of finding of these studies.

The next section offers recommendations from this study and gives concluding remarks.

6. Conclusions

The article reported about the behaviour of tertiary students regarding mobile device security as seen in literature and in a survey done that was part of a bigger study (Park 2014).
Recommendations and guidelines deducted from the results of the survey can be summarized as follows:

- The respondents often install new applications on their mobile devices. They should be made aware of the license agreements and be educated about reading the security messages when installing new apps.
- The respondents indicated that they often mix personal and business/other data on their mobile devices. They should be educated about this matter and be trained to use encryption for certain types of data – e.g. financial and other categories of sensitive data.
- The issue of active location services should be put into perspective to the tertiary students so that they know when to use it and only when absolutely necessary.
- Tertiary students should be made aware of how to protect their mobile devices. It seems that tablets are not as adequately protected as their PCs and smartphones.
- Specific protection mechanisms could be part of the educational efforts to teach tertiary students the types of protection and how to install and update these mechanisms such as encryption, antivirus programs etc.
- Act with caution when downloading online contents on the mobile device – thereby take responsibility for own actions and reducing risky behaviour.

In the introductory section the research aim was stated to describe the behaviour of tertiary students regarding mobile device security in order to learn from the study. It was seen in the results that certain aspects need more attention (e.g. read security messages) and in certain areas the respondents are reasonably security minded (e.g. adoption rates of protection mechanisms).

The contribution of this research is that users can be made more aware of mobile device security by assessing their behaviour, attitude and knowledge. Users must be aware of the potential security threats when using their mobile devices and must be mindful to apply security measures to protect themselves and their organizations. Focused educational efforts can assist in this regard taking into account the recommendations given to avoid risky behaviour.

References

Al-Hadadi, M. and Al Shidhani, A. (2013). Smartphone security awareness: Time to act. (In Proceedings of the 2013 International Conference on Current Trends in Information Technology, CTIT 2013, p. 166-171).

Allam, S., Flowerday, S.V. and Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42:56-65.

Anderson, J., Bonneau, J. and Stajano, F. (2010). Inglorious Installers: Security in the Application Marketplace. (In Proceedings of the 9th Workshop on the Economics of Information Security (WEIS'10)).

Androulidakis, I. and Papapetros, D. (2008). Survey Findings towards Awareness of Mobile Phones' Security Issues, Recent Advances in Data Networks, Communications, Computers, (In Proceedings of 7th WSEAS International Conference on Data Networks, Communications, Computers (DNCOCO'08), p. 130-135).

Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S. and Wolf, C. (2011). Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices, (In Security and Privacy (SP), 2011 IEEE Symposium on 2011, p. 96-111).

Benenson, Z., Hintz, N., Kroll-Peters, O. and Krupp, M. (2012). Poster: Attitudes to IT-Security When Using a Smartphone, *Eighth Symposium on Usable Privacy and Security (SOUPS)* 2012.

Böhme, R. and Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. (In Proc. of the 28th international conference on human factors in computing systems (CHI '10), ACM, USA, p. 2403–2406).

Botha, R.A., Furnell, S.M. and Clarke, N.L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security,* 28(3-4):130-137.

Drevin, L., Kruger, H.A. and Steyn, T. (2007). Value Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment. *Computers and Security,* 26(1):36-43.

Field, A.P. (2009). Discovering statistics using SPSS : (and sex and drugs and rock 'n' roll). Los Angeles ; London : SAGE; 3rd ed.

Gardezi, A.I. (2006). Security in wireless cellular networks. http://www.cse.wustl.edu/~jain/cse574-06/cellular_security.htm Date of access: 12 March 2015.

Harris, M.A., Furnell, S. and Patten, K. (2014). Comparing the mobile device security behavior of college students and information technology professionals. *Journal of Information Privacy and Security*, 10(4):186-202.

Harris, M.A. and Patten, K.P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security,* 22(1):97-114.

Heinrichs, L.R. and Jones, B.H. (2013). Tools and tips for teaching smartphone security. *Issues in Information Systems,* 14(2):329-335.

Jones, B.H., Chin, A.G. and Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends*, 58(6):73-83.

Kassin, S., Fein, S. and Markus, H. (2008). Social Psychology. Belmont: USA: Wadsworth.

Kline, P. 2000. The handbook of psychological testing. London : Routledge, 2nd ed.

Kruger, H.A. and Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers & Security,* 25:289-296.

La Polla, M., Martinelli, F. and Sgandurra, D. (2013). A survey on security for mobile devices. *IEEE Communications Surveys and Tutorials*, 15(1):446-471.

Landman, M. (2010). Managing smart phone security risks, (In Proceedings of the 2010 Information Security Curriculum Development Annual Conference, InfoSecCD'10 2010, p. 145-155).

Lawton, G. (2008). Is It Finally Time to Worry about Mobile Malware? *Computer,* 41(5):12-14.

Motiee, S., Hawkey, K. and Beznosov, K. (2010). Do Windows users follow the principle of least privilege? Investigating user account control practices. (In Proceedings of the 6th symposium on usable privacy and Security (SOUPS '10), ACM, USA , p. 1–13).

Mylonas, A., Kastania, A. and Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, 34:47-66.

Mylonas, A., Tsoumas, B., Dritsas, S. and Gritzalis, D. (2011). A secure smartphone applications roll-out scheme. (In Proceedings of the 8th International Conference on Trust, Privacy & Security in Digital Business, Springer, France, p. 49–61).

Oates, B.J. (2006). Researching information systems and computing. London: SAGE.

Ophoff, J. and Robinson, M. (2014). Exploring end-user smartphone security awareness within a South African context *Information Security for South Africa (ISSA),* 1-7.

Orlikowski, W.J. and Baroudi, J.J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information systems research*, 2(1):1-28.

Ott, D. (2014). Android* Security: Issues and Future Directions. *Intel Technology Journal*, 18(2):34-49.

Park, M. (2014). Mobile device security: Young people's awareness and perceptions. Research proposal MSc, North-West University, Potchefstroom. S.A.

Peng, S., Yu, S. and Yang, A. (2014). Smartphone malware and its propagation modeling: A survey. *IEEE Communications Surveys and Tutorials*, 16(2):925-941.

Robinson, T. (2014). Study reveals only 56 percent of employees get awareness training. SC Magazine. http://www.scmagazine.com/study-reveals-only-56-percent-of-employees-get-awareness-training/article/342029/ Date of access: 4 Feb 2015.

Shoemaker, D. and Conklin, W. (2012). Cybersecurity: The essential body of knowledge. Boston: USA: Cengage.

Tavakol, M. and Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, 2:53-55.