Security Awareness in Mobile Computing Devices Among Students of Higher Learning Institutions in Tanzania

By

Peter Elia Mosha[*]

Department of Population Studies, Institute of Rural Development Planning, Tanzania

[*]**Corresponding author:** pmosha@irdp.ac.tz

and

Stephen Method Lugaimukamu

Department of Development Finance and Management Studies (DFMS), Institute of Rural Development Planning, Tanzania

Abstract

The study on understanding the level of security awareness in mobile computing devices among students of Higher learning Institution in Tanzania; was conducted in Arusha region, involving; Institute of Accountancy Arusha, Mount Meru University and Arusha University. Asample of 327 students who were interviewed using questionnaires. The study results revealed that students possess little security awareness on threats and security features on the computing devices they use. Among those who were knowledgeable about the security features identified, some did not use these features and even those who used the featured yet some did not use these security features all the time. The study recommended that higher learning institutions should put in place guidelines, policies and artifacts to ensure security to students and institution community at large.

Keywords: *Mobile technologies, mobile devices, Tanzania, Security Awareness*

1. Background

Mobile computer devices are devices designed to be portable, often to fit on our lap, in the palm of our hand or in our pocket. With these mobile devices, one can do many of the things you do with a desktop computer while you are away from your working area or traveling. Features in mobile computer devices include batteries, video camera, camera, voice recorder and music player. The devices are mostly grouped into Laptop computers, tablets, smartphones, e-readers and handheld gaming devices, used to connect to the Internet and communicate with others.

The benefits of mobile devices are numerous and have been documented widely in various literature Eschenbrenner. and Nah, (2007); Lucas, (2016); Vats (2009) and Worthofusr (2015). Such benefits are across cutting in the sense that anyone using a smartphone device can realize them irrespective of their gender, ethnicity, religion, or educational background. The world has found itself pushing harder into the invention of new technology due to the need of its users requiring smaller, faster, portable devices (Wang et al., 2012). Manufacturers are required to produce hand-held mobile devices that are more affordable in terms of cost and are capable of performing all the functions that were initially being done by personal computer. These mobile devices are more prone to digital attacks as they are most of the time connected to the internet, occasionally without the knowledge of the user.

It has been found that there's growing rate of acceptance and usage of this mobile devices in higher learning studies, whereby for students, use this mobile devices mainly smartphones in their daily life at their universities. As Kafyulilo (2014) stipulated that mobile devices are more portable to carry, easy of reading and accessing contents, to the level that there is no need for you to open and close using like laptop computers, capability to have free/low cost software as well as data collection or note taking. Accomplishing these and many other tasks in a smart mobile device requires constant connection to the internet or network. In such cases, protection become number one priority as mobile computing devices are prone to several cyber-attacks such Spoofing, Denial of service, network congestion, spam, eavesdropping; loss, theft, disposal or damage; cloning SIM card; technical failure of device; unauthorized device (physical) access; unauthorized Access; offline tempering; crashing; misuse of phone identifiers and many more.

Security awareness is explained in different ways; such as Information Security awareness as an end-users general knowledge about information security and their consequences Ophoff, and Robinson (2014; Colwill (2009). According to Ophoff, and Robinson (2014) as cited in Kissel (2013) information security can be defined as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

While computer security threats are known to its users, the level of awareness of the security issues is little known to smartphone users. Sari and Candiwan (2014). Affordability of smartphones and their ubiquity exposes its user base to various security threats, as many users are being connected online through their smartphones. These means that users of smartphones are exposed to the threat of remotely being monitored or phishing of some of their information remotely without their knowledge by using some of the malicious software Felt et al (2011). Huang et al (2011) stipulated that when you increase user knowledge you can improve acceptance with good security practices. Parker et al(2015) "…proposed that user education using a simple, non-technical design is key to encourage security awareness and adoption of security controls, especially in emerging markets." Researches on mobile computing devices have largely been focusing on the adoption and security in installation of software packages from official repositories Mylonas et al (2013). Therefore, this study sought to understand the level of awareness about security features available in mobile computing devices among students of higher learning institutions in Tanzania: specifically finding out the level of awareness about security features available in smartphones, and examining the extent that students utilize these security features available in their smartphones.

2. Methods

Data for the study were collected from three higher learning institutions Institute of Accountancy Arusha (IAA), Mount Meru University and Arusha University, in Arusha city, Northern part of Tanzania, Africa. These academic institutions were used as a case representing several other institutions in this part of the country.

2.1. Study Design

The study used mixed approach, quantitative and qualitative approach which was expected to easy understanding of mobility, strength, flexibility, evolution, targeting on individual student behavior, on the awareness on mobile phone usage and security. The study design also intended to maintained a minimal interaction with the research participants when carrying out this study Wilson (2010). The target population were the students using smartphones in both undergraduate and postgraduate programs of the said institutions as they are most users who are likely to be very interested with this technology (MCD), and always interested in trying every new technology especially when it comes to new smartphones. Given these characteristics, students are more likely to be victims, and exploring what they know about security awareness on smartphone will enable them to use these devices at a safer way.

The study used a samplesize of 327 students in all the institutions mentioned which were sampled using convenience non-probability sampling technique.

2.2. Data collection and Analysis

The study used both primary and secondary data to ensure the findings of the study are as detailed as possible. Structured questionnaires which was mainly multiple-choice questions were used as they are said to be good way of evaluation method especially when surveying user's practices. The filled questionnaire was returned to the researcher through personal delivery or through e-mail.

Collected data were carefully coded and entered into IBM SPSS Statistics software version 20, which was used to clean, manipulate and analyse the data. Descriptive statistics was the main analysis technique that was used where categorical answers frequencies were tabulated while for qualitative data mean and other measures of dispersion a were assessed.

3. Findings and Discussions

3.1. Participants Personal characteristics

The data was collected main from male and female students with a bit more males when compared to female given the enrolment status of more male students in higher learning Institutions. Data released that more than two-third of all interviewed students were of the age between 18 to 29 (72%) years followed by those who were between 30 years to 39 (%). Data also revealed that students interviewed were studying accounting, logistic, business, computing and education studying at bachelor level mainly (54%) followed by diploma (31%).

Table 1: Participants Characteristics

Characteristic	Frequency	%
Male	*187*	*57*
Female	*140*	*43*
Age group		
Under 18 years	*2*	*1*
18-29 years	*237*	*72*
30-39 years	*67*	*20*
40-49 years	*17*	*5*
50-59 years	*3*	*1*
Above 60 years	*1*	*0*
Area of study		
Accounting	*124*	*38*
Business	*63*	*19*
Logistics	*34*	*10*
Computing	*91*	*28*
Education	*15*	*5*
Level of study		
Certificate	*20*	*6*
Diploma	*101*	*31*
Bachelor	*177*	*54*
Post-graduate	*20*	*6*
Masters	*9*	*3*

During the study students were asked to respond on what information do they use their smart phones to access and the results revealed that most students mostly use their mobile computing devices to store and keep their personal data (20%) access social media platforms (18%), Used as storage devices by inserting memory card (16%), accessing and reading their class related notes (14%); also mentioned that they use these mobile computing devices in accessing bank information and making other financial transactions (11%). It was again reported some used the mobile devices to install and access computer applications (10%)

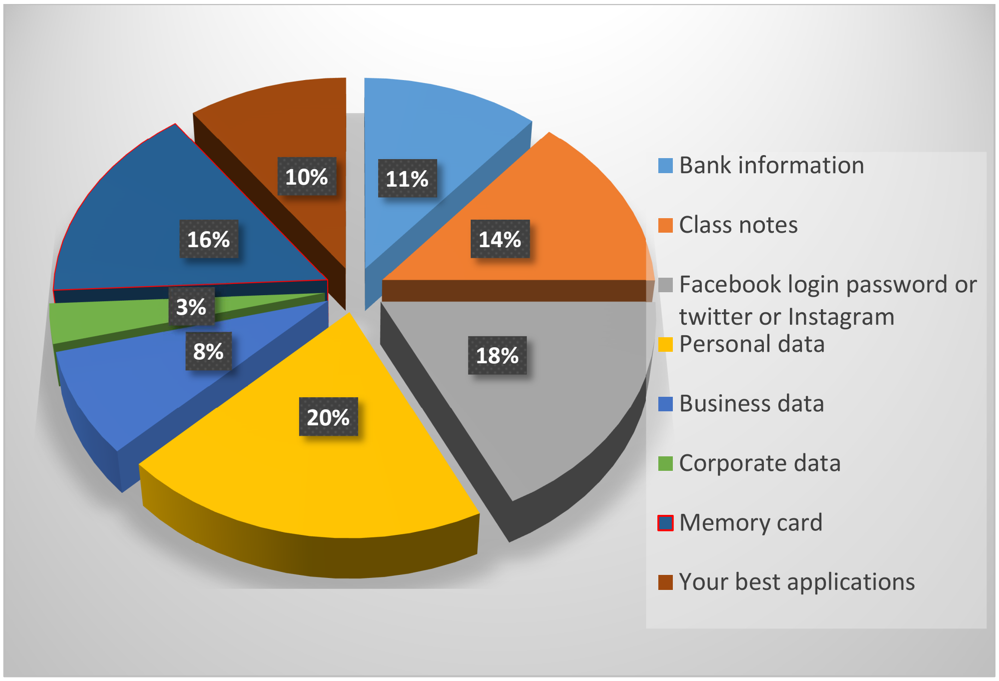

Figure 1: Uses of Mobile Computing Devices

The findings on the above figure shows that there's no great variation between what they store on their smartphone when looking on social media such as Facebook, Twitter or Instagram; personal data and possession of memory card. But some use for class notes storage showing that smartphone are useful in simplifying their studies. There's great danger that 11% of the students store bank information which can be a great risk once someone hack their smartphone, if he/she does not possess the knowledge of security features present in their smartphone.

The study also assessed the Operating System of Mobile Computing Devices Owned by Participants. The operating system used is believed to directly relate to the awareness and level of securing that the customer will secure.

Table 2: Operating System Popularity

Operating System	Sample popularity	Order of popularity
Android	*81.7%*	*1*
Blackberry	*3.7%*	*4*
Symbian	*0.6%*	*5*
Windows mobile	*4.9%*	*3*
iPhone iOS	*8.0%*	*2*
Bada	*0.3%*	
Palm OS	*0.3%*	
Sailfish OS	*0.3%*	
Maemo	*0.3%*	

Source: Research Data (2016)

The results in Table 2 revealed to a very large extent (81.7%) many of participants use Androids when compared to other operating systems, which shows that 8.0%, 4.9%, 3.7% and 0.6%, of participants use iPhone iOS, Windows mobile, Blackberry, and Symbian respectively. There are a number of reasons related to use of Android operating system including easiness to use, less expensive and it's technology is open source. This was also reported by study done by Mylonas et al (2013), which provided the same similarity.

3.2. Level of awareness about security features available in mobile computing devices among students of higher learning institutions

Given the undeniable explosion and rapid spread of smartphones and other mobile devices coupled with their persistent, routine use, universities/college students must exercise vigilance in mobile device security. This awareness necessity is crucial to all institutions of higher education, which are a stomping ground for a massive population of fearless and hungry consumers of every new technology. Students in these higher learning institutions need to be aware of risks attached with use of mobile computing devices that they use in day to day learning and campus life. Data collected revealed that many students were concerned (64.8%) about security issues while about one-third of the students were undecided about security issues. Descriptively the data showed that many students were concerned with security of the information/data stored in their mobile devices ($Mean = 2.13, Median \ = 2.00 \ and \ Standard \ deviation = \ .886$). It is right to say, having almost one-third of college students not being aware and showing less concern for mobile computing devices security risks is not few number. Cate (2006) reported that Institutions of higher education pose increased temptation and security risk for these institutions "possess a large volume and variety of sensitive information on a wide range of individuals, and demands for this information are growing.

Table 3: Level of security concern among student in Higher Learning Institutions

Levels of Security Concern	**Frequency**	**Percentage**
Extremely concerned	*90*	*27.5*
Concerned	*122*	*37.3*
Neutral	*103*	*31.5*
Not concerned	*8*	*2.4*
Extremely not concerned	*4*	*1.2*
Total	*327*	*100.0*

Source: Research Data (2016)

Students uses Mobile devices, particularly smartphones, which surely have a powerful and significant presence on campuses and are used not just for social communication (Gikas and Grant, 2013), but they are increasingly using these mobile devices for access to academic material, submission of work, online research downloading and storing their results, and for financial transactions. Likewise, these devices, even more so than other PCs (Wong et al., 2015), are used for surfing on and interacting with websites, where a variety of security breaches including cross-site scripting (Hydara et al., 2015; Johns, 2014) occurs. The study further assessed level of understanding of student towards these security threats and results are shown in Table 4.

Table 4: Level of Students Understanding on Existence of Security Threats

Threat	Level of Understand on threats				
	Very good	Good	Fair	Poor	Very poor
Spoofing	32(12.6)	71(28.8)	61(24.0)	41(16.1)	49(19.3)
Scanning	77(27.8)	97(35.0)	66(23.8)	21(7.6)	16(5.8)
Denial of service, network congestion	59(22.5)	94(35.9)	65(24.8)	17(6.5)	27(10.3)
Spam, Advertisements	53(20.7)	94(36.7)	57(22.3)	28(10.9)	24(9.4)
Eavesdropping	18(8.1)	52(23.4)	60(27.0)	51(23.0)	41(18.5)
Jamming	37(15.9)	45(19.3)	74(31.8)	43(18.5)	34(14.6)
Loss, theft, disposal or damage	65(25.1)	68(26.3)	55(21.2)	42(16.2)	29(11.2)
Cloning SIM card	47(19.4)	66(27.3)	58(24.0)	41(16.9)	30(12.4)
Technical failure of device	35(14.1)	76(30.5)	68(27.3)	41(16.5)	29(11.6)
Unauthorized device (physical) access	38(5.0)	77(30.3)	71(28.0)	38(15.0)	30(11.8)
Unauthorized Access	39(15.4)	88(34.6)	57(22.4)	43(16.9)	27(10.6)
Offline tempering	25(10.5)	72(30.4)	57(24.1)	48(20.3)	35(14.8)
Crashing	35(14.3)	50(20.4)	73(29.8)	45(18.4)	42(17.1)
Misuse of Phone Identifiers	29(12.5)	56(24.1)	66(28.4)	46(19.8)	35(15.1)
Electrical tracking/surveillance/exposure of physical location	51(19.4)	77(29.3)	60(22.8)	46(17.5)	29(11.0)
Resource abuse	32(12.7)	58(23.0)	68(27.0)	49(19.4)	45(17.9)
Sensitive Information Disclosure (SID), Spyware	26(10.4)	68(27.1)	70(27.9)	47(18.7)	40(15.9)
Corrupting or modifying private content	35(13.9)	62(24.7)	82(32.7)	35(13.9)	37(14.7)
Disabling applications or the device	44(17.7)	69(27.8)	73(29.4)	33(13.3)	29(11.7)
Client side Injection/Malware	32(12.9)	65(26.1)	60(24.1)	50(20.1)	42(16.9)
Direct billing	23(9.3)	64(26.0)	69(28.0)	42(17.1)	48(19.5)
Phishing	26(10.2)	54(21.3)	55(21.7)	61(24.0)	58(22.8)

Students involved in this study revealed partial understanding about various security threats listed in the questionnaire used. Data shows most students only have high awareness on issues of scanning their devices (62.8%), denial service, and network congestion (58.4%) and spam and advertisements (57.4%). If combine all those who showed very good and good level of understanding and compare them to those who showed fair, poor and very poor understanding, plotting their percentage in a line graph it shows most students below average understanding of mobile device threats (see figure 2). These results are in line with the results of a study done by

Chin et al (2012), showing most users are concerned about security on their smartphone than on their laptops. But the study done by Ophoff and Robinson (2014) shows rarely concern about security. This kind of concerned shown by the participants on this study, does not reflect on the knowledge of security threats as seen on the followed discussion on knowledge on the security threats.

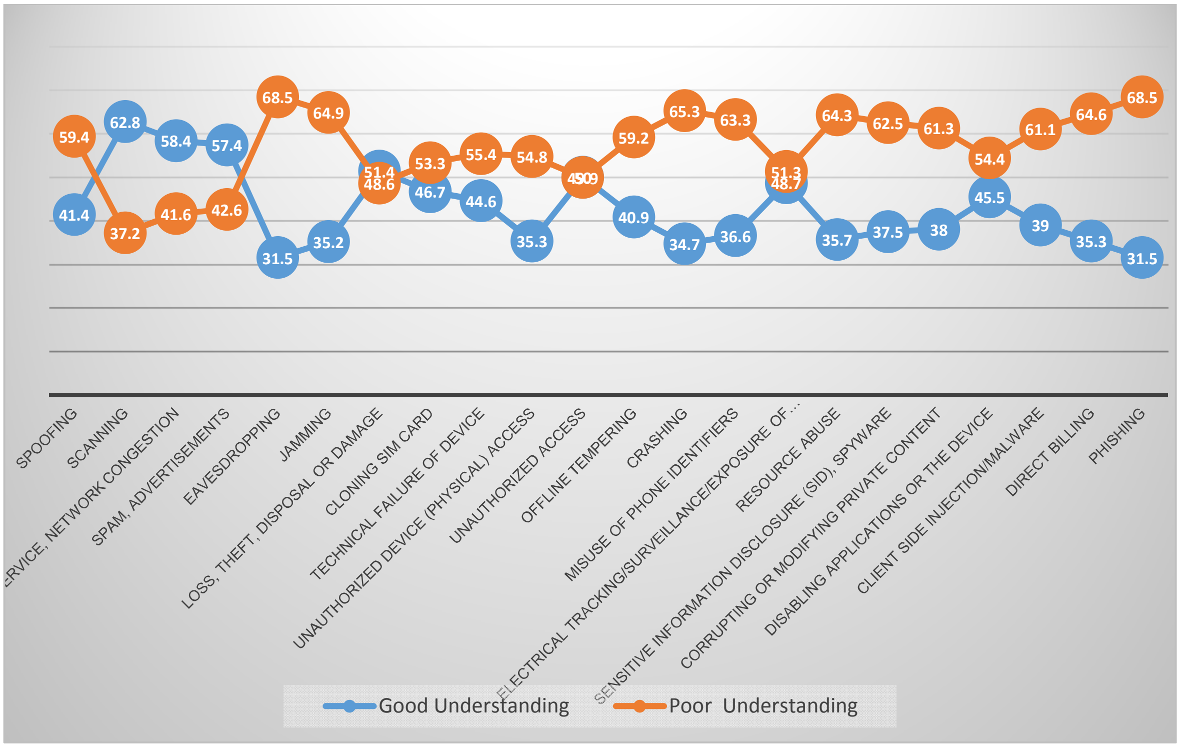

Figure 2: % Level of Understanding the existence of Mobile Computing Devices Threats

3.3.Knowledge of Security Features and Usage in Mobile Devices

The study assessed the knowledge of students on security features present in their mobile devices and compare the known features again if they use the features or not. The data in table 5 are from 327 participants and displayed a $Median = 3.0000$knowledge of security features ($IQR = 2.0$. The data shows students knows various security features in their mobile devices, but usage of these features is low when compared to number (%) of those who knows the features. It is a security concern when someone is aware and knows how to use certain security feature. This substantial usage and penetration into mainstream daily life renders knowledge of and adherence to appropriate security measures and practices vital.

Table 5: Feature you known and used in protecting Mobile Devices among Higher learning Students

Security Features	Tick	
	Know	Use
Auto-Lock or automatically lock	263(77.6)	189(60.4)
Lock Screen (PIN, Password)	290(85.5)	220(70.3)
Pattern lock	289(85.3)	190(60.7)
Power button instantly lock	233(68.7)	123(39.3)
SIM card lock/SIM PIN	243(71.7)	122(39.0)
Password of the device (Device PIN, Passcode lock)	231(68.1)	111(35.5)
facial recognition	198(58.4)	45(14.4)
Fingerprint	217(64.0)	66(21.1)
Unknown sources	188(55.5)	49(15.7)
Device administrator	184(54.3)	70(22.4)
Verify Apps	203(59.9)	93(29.7)
App permission	198(58.4)	104(33.2)
Safety Wi-Fi, Bluetooth or NFC	220(64.9)	132(42.2)
Encryption phone	194(57.2)	68(21.7)
Encryption Application (App Lock)	201(59.3)	84(26.8)
Mobile anti-theft	200(59.0)	74(23.6)
Store and backup data	224(66.1)	146(46.6)

The findings obtained from Table 5, the understanding of these security features were not known by most of the students (participants) and confirmed similar findings in previous study such as that of Mylonas, Kastania, and Gritzaliss (2013), Parker, Ophoff and Van Belle (2015) and Jones, and Heinrichs (2012), but the study done by Sari, and Candiwan (2014) show the opposite where by users have the higher level of knowledge about security threats. As said on the level of concern about security which showed that participants are concern about security, but have little knowledge about the security threats, but again those with knowledge about the features still some did not use the known features. This shows that there's a desire to the participants to protect themselves but they have failed to have the knowledge and willingness on the security threats.

The study addressed the behavior on usage of features to find out how participants are frequently using the security features that are present on participants' mobile devices as to tackle the security threats. It was found from the data that out of 326 participants in the studied sample displayed a $Median = 3.0000$ behavior on usage of features($IQR = 3.00$)whilein the other hand the results displayed in figure 3 gives more detail whereby the horizontal line indicate the median, and the box covers the inter quartile range by displaying the spread of participants along selected choices. The spread is concentrated from rarely to always for most of the participants.

The findings on the figure 3 relate how frequently participants use security features present on their mobile computing device and the data present that most of the participants are not using the mentioned security features every time even though they know these features. This also is seen on the study conducted by Mylonas et al (2013) and Jones, and Heinrichs (2012). So there's a great chance of users to find themselves being victims of cybercrimes or facing security threats on their mobile devices. This may imply that there is need for more training on awareness of the security threats and how such security features can protect users against particular threats.

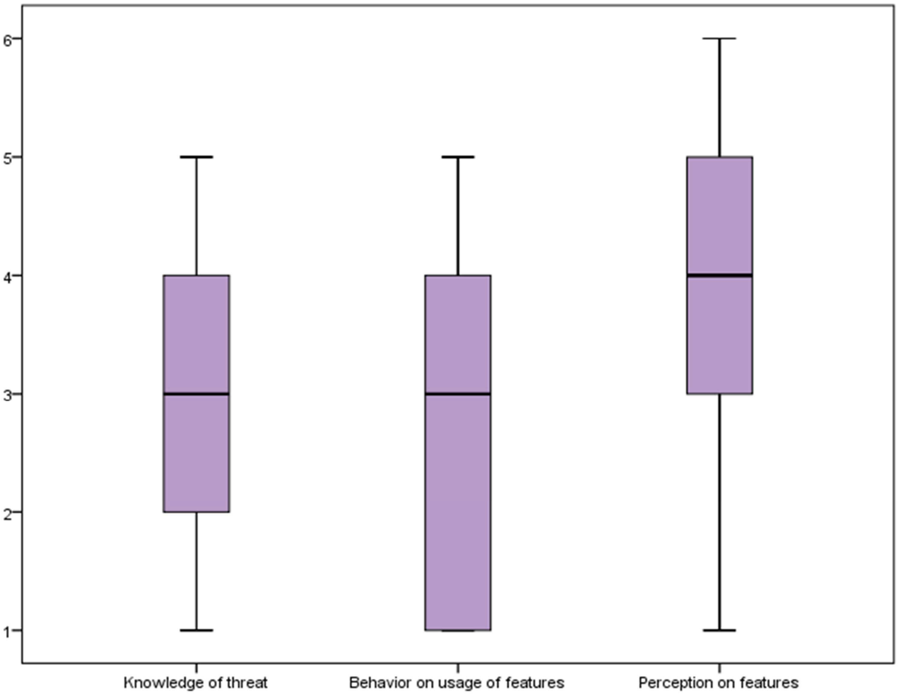

Figure 3: Knowledge of threat, Behavior on Using and Perception on Security features

4. Conclusion and Recommendations

4.1. Conclusion

There has been a world-wide concern over the security concerns of mobile computing devices used among higher learning institutions. The study involved assessed level of awareness about security features available in mobile computing devices among students of higher learning institutions in Tanzania. Collected data unveiled that students in the study are concerned about security of their mobile computing devices. The data also revealed that there is little knowledge on the security threats, and most participants use this security features not all the time. Therefore, all these can be concluded, that participants have partial knowledge and then partial use over security features and thus why a little number of participants use the security features rarely and even sometime do not use some of the features at all.

4.2. Recommendations

Following the findings from this study and various reviewed studies in relation to this study summarized in this article about Security awareness in Mobile Computing Devices among Students of Higher Learning Institutions in Tanzania, the following are recommended:

- Given the universal usage of mobile computing devices and their unmitigated penetration into academia, institutions of higher education must establish short and thorough mobile security policies and then, must actively emphasize compliance from the university community.
- Higher learning institutions should train students on identification and use of basic security features for mobile computing devices to help protect the rich assortment of sensitive data mainly stores and accessed by student through these devices.
- This study did not examine the language as an aspect that impact security awareness, or between IT experts and non IT experts. Therefore, this can be the basis for future related research.

REFERENCES

1. Ajzen, I., 1991. The theory of planned behavior. Organizational behavior and human decision processes, 50(2), pp.179-211.

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

3. Buchoux, A. and Clarke, N.L., 2008, January. Deployment of keystroke analysis on a smartphone. In Australian Information Security Management Conference (p. 48).

4. Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), pp.523-548.

5. Cate, F. H. (2006). The Privacy and Security Policy Vacuum in Higher Education. Educause Review, 41(5), 18.

6. Chin, E., Felt, A.P., Sekar, V. and Wagner, D., 2012, July. Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security (p. 1). ACM.

7. Colwill, C., 2009. Human factors in information security: The insider threat–Who can you trust these days?. Information security technical report, 14(4), pp.186-196.

8. Davis, F.D., Bagozzi, R.P. and Warshaw, P.R., 1989. User acceptance of computer technology: a comparison of two theoretical models. Management science, 35(8), pp.982-1003.

9. Dawson, C 2002, Practical Research Methods: A user-friendly guide to mastering research, How To Books Ltd, 3 Newtec Place, Magdalen Road, Oxford OX4 1RE, United Kingdom.

10. Dudovskiy, J. 2013, "The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance", viewed 30 July 2016, http://research-methodology.net/research-methodology/

11. Eschenbrenner, B. and Nah, F.F.H., 2007. Mobile technology in education: uses and benefits. International Journal of Mobile Learning and Organisation, 1(2), pp.159-183.

12. Esmaeili, M., 2014, 'Assessment of Users' Information Security Behavior in Smartphone Networks' Master's Theses and Doctoral Dissertations. Paper 581, Eastern Michigan University, DigitalCommons@EMU

13. Fishbein, M. and Ajzen, I., 1977. Belief, attitude, intention, and behavior: An introduction to theory and research.

14. Gikas, J. & Grant, M. (2013). Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones & social media. Internet and Higher Education, 19, 18-26.

15. Golafshani, N., 2003. Understanding reliability and validity in qualitative research. The qualitative report, 8(4), pp.597-606.

16. Huang, D.L., Rau, P.L.P., Salvendy, G., Gao, F. and Zhou, J., 2011. Factors affecting perception of information security and their impacts on IT adoption and security practices. International Journal of Human-Computer Studies, 69(12), pp.870-883.

17. Hydara, I., Sultan, A., Zulzalil, H., & Admodisastro, N. (2015). Current state of research on cross-site scripting (XSS) – A systematic literature review. Information and Software Technology, 58, 170-186. doi:10.1016/j.infsof.2014.07.010

18. Jeon, W., Kim, J., Lee, Y. and Won, D., 2011, July. A practical analysis of smartphone security. In Symposium on Human Interface (pp. 311-320). Springer Berlin Heidelberg.

19. Johns, M. (2014). Script-templates for the Content Security Policy. Journal of Information Security and Applications, 19, 209-223. doi:10.1016/j.jisa.2014.03.007

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

21. Jones, B.H. and Heinrichs, L.R., 2012. Do business students practice smartphone security?. Journal of Computer Information Systems, 53(2), pp.22-30.

22. Kafyulilo, A., 2014. Access, use and perceptions of teachers and students towards mobile phones as a tool for teaching and learning in Tanzania. Education and Information Technologies, 19(1), pp.115-127.

23. Kataria, A., Anjali, T. and Venkat, R., 2014, February. Quantifying smartphone vulnerabilities. In Signal Processing and Integrated Networks (SPIN), 2014 International Conference on (pp. 645-649). IEEE.

24. Kothari, C.R. (2004) Research Methodology: Methods and Techniques 2nd Ed. New Delhi, India: New Age International (P) Limited.

25. Landman, M., 2010, October. Managing smartphone security risks. In 2010 Information Security Curriculum Development Conference (pp. 145-155). ACM.

26. Lauesen, S. and Younessi, H., 1998, June. Six Styles for Usability Requirements. In REFSQ (Vol. 98, pp. 155-166).

27. Leslie J. and Walker, S.J, 1910, ‘Theories of Knowledge Absolutism Pragmatism Realism’, Longmans, Green & Co., 39 Paternoster Row, London, New York, Bombay, and Calcutta, viewed 13 August 2016, https://www3.nd.edu/~maritain/jmc/etext/walker.htm

28. Lucas, 2016, ‘Advantages and Disadvantages of Mobile Phones’, viewed 13 August 2016, http://www.enkivillage.com/advantages-and-disadvantages-of-mobile-phones.html

29. Merriam-Webster, ‘Knowledge’, (n.d.). Retrieved August 13, 2016, from http://www.merriam-webster.com/dictionary/knowledge

30. Mylonas, A., Kastania, A., and Gritzalis, D., “Delegate the smartphoneuser? Security awareness in smartphone platforms,” Computers &Security, vol. 34, pp. 47–66, May 2013.

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

32. Parker, F., Ophoff, J., Van Belle, J.P. and Karia, R., 2015, November. Security awareness and adoption of security controls by smartphone users. In 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec) (pp. 99-104). IEEE.

33. Peraković, D., Husnjak, S. and Remenar, V., 2012, January. Research of security threats in the use of modern terminal devices. In 23rd International DAAAM Symposium Intelligent Manufacturing & Automation: Focus on Sustainability.

34. Pfleeger, S.L. and Kitchenham, B.A., 2001. Principles of survey research: part 1: turning lemons into lemonade. ACM SIGSOFT Software Engineering Notes, 26(6), pp.16-18.

35. Sari, P.K. and Candiwan, C., 2014. Measuring Information Security Awareness of Indonesian Smartphone Users. TELKOMNIKA (Telecommunication Computing Electronics and Control), 12(2), pp.493-500.

36. Saunders, M, et al (2007) Research Methods for Business Students 4th ed. Harlow: Pearson Education Limited

37. Security Awareness Program Special Interest Group PCI Security Standards Council n.d, Best Practices for Implementing a Security Awareness Program, PCI DSS, October 2014, version 1.0, viewed 15 August 2016 https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

38. Simon, M. K. (2011). Dissertation and scholarly research: Recipes for success (2011 Ed.). Seattle, WA, Dissertation Success, LLC. Viewed on 18 August 2016, http://dissertationrecipes.com/wp-content/uploads/2011/04/AssumptionslimitationsdelimitationsX.pdf

39. Theoryofknowledge.info, 2016, 'Theory of Knowledge' viewed 13 August 2016, http://www.theoryofknowledge.info/

40. TanzaniaInvest, 2016, 'Tanzania Mobile Subscriptions Increase by 24% in 2015 and Internet Penetration Reach 34%', viewed 13 August 2016, http://www.tanzaniainvest.com/telecoms/tanzania-mobile-subscriptions-reach-39-million-and-internet-penetration-reach-34-percent-in-2015

41. U.S. Dept. of Health and Human Services. The Research-Based Web Design & Usability Guidelines, Enlarged/Expanded edition. Washington: U.S. Government Printing Office, 2006, viewed 15 August 2016, https://www.usability.gov/what-and-why/usability-evaluation.html

42. Vats, A 2009, ‘1o benefits of cell phones!’, Latest Technology Blog, web log post, March 21, 2009, viewed from 13 August 2016, http://www.techacid.com/2009/03/21/1o-benefits-of-cell-phones/

43. Wang, Z., Johnson, R., Murmuria, R. and Stavrou, A., 2012. Exposing Security Risks for Commercial Mobile Devices. Computer Network Security, pp.3-21.

44. Wilson, J. (2010) “Essentials of Business Research: A Guide to Doing Your Research Project” SAGE Publications

45. Wong, K., Wang, F., Ng, K., Kwan, R. (2015). Investigating Acceptance towards Mobile Learning in Higher Education Students, *Technology in Education. Transforming Educational Practices with Technology,* Volume 494 of the series Communications in Computer and Information Science, 9-19.

46. Worthofusr, May 18, 2015 ‘Advantages and Disadvantages of Mobile Phones for Students’, viewed 13 August 2016, http://www.worthofread.com/advantages-and-disadvantages-of-mobile-phones-for-students/

47. Zefferer, T. and Teuf, P., 2011. Opportunities and forthcoming challenges of smartphone-based mgovernment services. Eduard Aibar, p.56.