Analysis of the Security Threat and Vulnerability of Smartphone use among Tertiary Students in Ghana

Issah Bala Abdulai[1], Abu Sulemana[2]

[1]Kibi Presbyterian College of Education, Department of Mathematics & ICT, Kibi, Ghana

[2]Al-Faruq College of Education, Department of Mathematics & ICT, Wenchi, Ghana

Abstract: *The study was to find out the extent at which tertiary students in Ghana use Smartphone, and to examine the level of awareness regarding security risks that accompany the use of smartphones among tertiary students. A cross-sectional survey design was employed to collect data in four tertiary institutions. Data was collected from 150 tertiary students. These tertiary students were randomly sampled during visits to the various institutions. Data was gathered through questionnaire for all participants. The data was analysed using frequency counts and percentages to answer research questions. The results indicated that, generally, most tertiary students in Ghana use android operating system smartphones. Besides, some of the tertiary students are not aware of the security threat and vulnerability that affect their smartphones. Furthermore, majority of the tertiary students in Ghana do not do enough to protect their smartphone from being attacked. Finally, the study suggests a training programme to equip the tertiary students to manage the threat efficiently.*

Keywords: Smartphone, Security Risk, Information Security, Operating System, Vulnerability

1. Introduction

The new trends in mobile technologies have brought a new kind of device known as the smartphone. Smartphones are equipped with various operating systems just like those on notebook or desktop computers. These operating systems range from Android, iOS, windows, among others. These trends make smartphone operating systems vulnerable to many of the same threats as notebook and desktop operating systems.

Many mobile phone users have shifted their passion to smartphones and among these passionate users are tertiary students. The widespread adoption of mobile technologies has dramatically affected the landscape of conducting research, particularly survey researchers [2], and those focusing on tertiary students are no exception. Research has shown that smartphone users, and university students in particular, are complacent when it comes to security behaviour in using smartphones [9][4][3].

Information security is considered as the act of protecting information as well as information systems from illegitimate access, usage, revelation, disruption, alteration, or destruction in order to obtain confidential report of an institution or an individual [6]. In view of this, most users perceive data stored on the smart devices to be private and worth protecting [13] [8].

1.1 Research Problem

Smartphones do not run uniform operating systems; as a result, each available operating system has its own unique attributes and employs different approaches regarding manipulation. Currently, there are many operating systems that come with smartphones; they include android, iOS, windows, symbian, and blackberry among others.

Smartphone application face many of the security threats as traditional computers due to varieties of operating systems, besides, they are prone to physical loss and theft, physical damage and are often improperly handle which results in these devices being of considerable risk [7]. Some of the threats that are similar to those of the traditional computers are malware, attacks on individuals, hacking and denial of service [4] [12]. These issues pose many questions that need to be answered. To what extend do the tertiary students use smartphones in their learning processes? Are the students aware of the threats involves in using smartphones? How do the students safeguard the threats? These questions among others require answers.

1.2 Objectives

The use of smartphones in tertiary institutions will continue to grow since they are considered as one of the emerging technologies in the 21st century. Besides, it is the largest device use by learners in teaching and learning processes globally, as such making it vulnerable to security threats since people are not aware of the challenges surrounding smartphone usage. The number of students using smartphones to access learning resources, store personal data among others will rise astronomically in due course. But they may not engage in practices that will minimize potential threats. In this regard, the objectives used for the analysis of the security threat and vulnerability of smartphone uses among tertiary students in Ghana are as follows:
a) To determine the extent at which tertiary students use smartphones in Ghana.
b) Examine the level of awareness of security risks that accompany the use of smartphones among tertiary students in Ghana.

2. Review of Related Work

Smartphones enable students to learn effectively because it reduces the time taking to get the content being taught through the interaction [10]. Smartphone usage also assists

students to compare abstract concept with concrete one which enhances learning. Additionally, [14] considered smartphones as being productive since it allows learners to improve on their academic performance. More so, smartphones are effective devices for note taking, and which promote students learning in an institution [1]. However, current research indicates significant benefits of smartphone uses for teaching and learning processes. Its major challenge to learning is when students use the device in playing games instead of learning [14].

Also [11], report that teachers and students elsewhere are worried about the threats to data security and privacy in respect to the use of Smartphone. Teachers who try to discuss these challenging. Issues often hide their identity as a protective measure from people who could harm them. Also, [5] identifies threats of smartphone as a learning tool to maintain security and privacy of data and system. The details are how to safeguard data stored on a smartphone; prevent illegal access, filtering the content, protection of data in the cloud, and protection of intellectual property. The major challenge has to do with deploying suitable security policies. The process of detecting, preventing malicious attacks, maintaining the integrity, privacy and confidentiality of the data stored in the smart phones is necessary.

3. Methodology

In order to better understand the level of smartphone security awareness of tertiary students, a descriptive survey was used, and a questionnaire was the main tool developed to assess students' demographics, extent of smartphone use and smartphone security awareness.

3.1 Data Collected

Demographics, including information such as course of study, age, gender and school attended were collected. The second section was on the level of smartphone security risks awareness among tertiary students in Ghana, and this consisted of 11 items. The participants were to respond to the statements by indicating either Agree or Disagree.

3.2 Study Limitations

The limitation of this study is that findings may be affected by the sample's demographics or groups. It could be that significant differences exist in the security awareness of smartphone users between different demographics or groups (e.g. different tertiary institutions).

The study sample size was very small. Only one hundred and fifty (150) students were selected from 4 tertiary institutions. This is not statistically representative of the student population in Ghana tertiary institutions. Also, the number of the responses were based on self-reported figures, and may be skewed since users may not indicate their actual level of usage or wish to conceal what they perceive to be sensitive.

Table 1: Descriptive statistics of Participants regarding Gender

Respondents	Frequency	Percentage
Male	81	54%
Female	69	46%
Total	150	100

In table 1, 81(54%) of the respondents were male students, while 69 (46%) were female students. This gives an indication that there were more males as compared to females in the sample of students used for the research.

Table 2: Descriptive statistics of Age of Participants

Age	Frequency	Percentage
19-21	40	26.7%
22-25	39	26.%
26-30	34	22.7%
Above 30	37	24.7%
Total	150	100

The analysis in table 2 shows that 40 (26.7%) of the respondents were within the 19-21 years' age bracket. Also, 39 (26%) were between 22-25 years, while 34 (22.7%) were between 26-30 years. Finally, 37 (24.7%) were above 30 years. This shows that majority of the students sampled were between 19-21 years, while the least participants were 50 years and above.

Table 3: Descriptive statistics of Courses offered by participant

Subject	Frequency	Percentage
Science and mathematics	28	18.7%
Languages	33	22%
Social science	24	16%
Education	20	13.3%
Humanities	45	30%
Total	150	100

Table 3 shows courses offered by the students in the sampled tertiary institutions. The number of students perusing Mathematics and Science is 28 (18.7%). Besides, languages are represented by 33 (22%), while 24 (16%) offered social science. Furthermore, 20 (13.3%) represent students studying education and 45 (30%) study humanities.

Table 4: Descriptive statistics of Institutions attended by participants

School	Frequency	Percentage
Kibi Presbyterian College of Education	40	26.7%
University of Ghana	34	22.7%
Koforidua polytechnic	37	24.7%
Sikkim Manipal University	39	26.%
Total	150	100

Table 4 indicates that 40 (26.7%) of the respondents attended Kibi Presbyterian College of Education, also, 34 (22.7%) from the University of Ghana, Legon while 37 (24.7%) attended Koforidua Polytechnic. Finally, 39 (26%) attended Sikkim Manipal University.

Table 5: Descriptive statistics of students' smartphones uses and operating systems

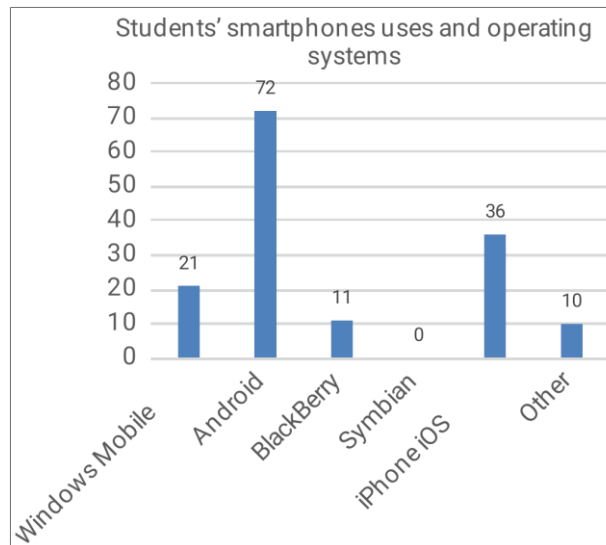| Operating system	Frequency	Percentage
Windows Mobile	21	14.0%
Android	72	48.%
BlackBerry	11	7.3%
Symbian	0	0
iPhone iOS	36	24%
Other	10	6.7%
Total	150	100

Figure 1: Shows a bar chart illustrating students' smartphones uses and operating systems

Results from table 5 and figure 1 shows 21 (14%) of the respondents use Windows Mobile smartphone, 72 (48%) use Android smartphone, 11 (7.3%) use Blackberry smartphone, 36 (24%) use iPhone iOS smartphone, none of the respondents use Symbian operating system and 10 (6.7%) use other operating system.

Table 6: Level of security awareness among participants

| S/N	Statement	Agree	Disagree	Total
1	The Applications in the official repository of my smartphone is safe to use?	102(68%)	48(32%)	150(100%)
2	I am concerned about the privacy and protection of my personal data on my smartphone.	108(72%)	42(28%)	150(100%)
3	I know what the term iPhone jail breaking means.	21(13%)	129(87%)	150(100%)
4	I prefer the installation of a pirated applications to buying the original applications.	93(62%)	57(38%)	150(100%)
5	I am aware of the existence of smartphone malicious software (virus, worm, Trojan horse, etc.).	66(45%)	84(55%)	150(100%)
6	I am aware of the existence of smartphone security software (e.g. antivirus, firewall,	72(48%)	78(52%)	150(100%)
7	I consider smartphone security software essential.	57(38%)	93(62%)	150(100%)
8	I have ever searched the application repository for free smartphone security software.	63(42%)	87(58%)	150(100%)
9	I store personal data on the smartphone.	117(78%)	33(22%)	150(100%)
10	I store business data on my smartphone	54(36%)	96(64%)	150(100%)
11	I have ever misplaced a smartphone.	48(32%)	102(68%)	150(100%)
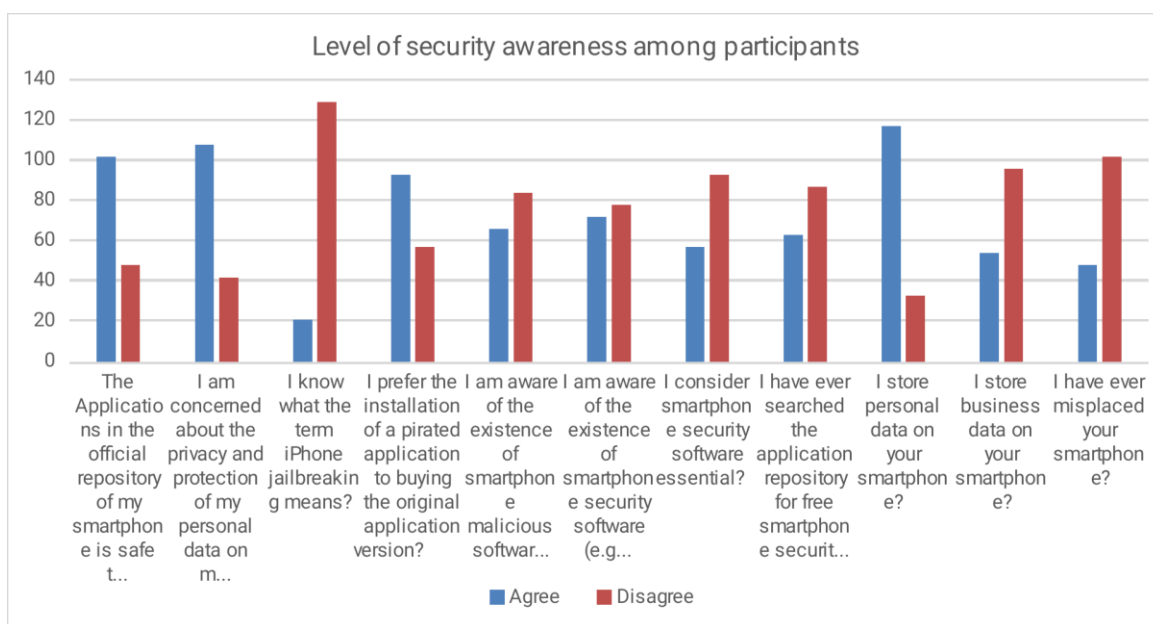
Figure 2: Shows the Level of security awareness among participants

From Table 6 and figure 2 indicates 102 (68%) of the respondents believed that applications downloaded from the application repository are secure. Also, it indicates that 108 (72%) are concerned about the privacy and protection of their personal data. In addition, 129 (87%) were not aware of the term jailbreak. Besides, 93 (62%) of the respondents prefer pirated applications from original ones. Majority of the respondents 84 (55%) are not aware of the existence of smartphone malicious software. Furthermore, evident from the result shows that 78 (52%) of the respondents were not aware of the existence of smartphone security software. More so, 93 (61%) consider smartphone security essential. Regarding the statement, if they ever searched the application repository for free smartphone security software, 87 (58%) responded positively to it. It is noted that 117(78%) stored personal data on their smartphones, while 54 (36%) store business data on their smartphones and 48 (32%) indicated they ever, misplaced their smartphones before.

4. Findings

The findings of the study are as follows:
1) Tertiary students' usage of smartphones in Ghana.
a) The results indicated that majority of the students in Ghanaian tertiary institutions use smartphone with android operating system.
b) The smartphones are used by both male and male students at the tertiary level in Ghana.
c) Also, students pursuing all programmes use smartphones in the instructions.
d) There is no age limit regarding the use of smartphones in the tertiary instructions.

2) The level of awareness of security risks that accompany the use of smartphones among tertiary students in Ghana.
a) It was found out that, most tertiary students in Ghana are concerned about the privacy and protection of their personal data on their smartphones.
b) Also, some tertiary students ever misplaced their smartphone before.
c) Most students are not aware of the existence of smartphone security software.
d) Finally, tertiary students in Ghana stored personal and business data on their smartphones.

5. Conclusions

The study was to find out how tertiary students use smartphones in Ghana. Besides, examine the level of awareness of security risks that accompany the use of smartphones among tertiary students in Ghana. The study concluded that students in the Ghanaian tertiary institutions use android operating system smartphone. Also, tertiary students in Ghana are concerned about the privacy and protection of their personal data on their smartphones. Besides, some tertiary students ever misplaced their smartphone before. All students use smartphones in the tertiary institutions, regardless of their age and sex. Finally, tertiary students are not aware of the existence of smartphone security software that could protect their phone efficiently.

6. Recommendations

From the analysis, the study recommends smartphone manufacturers to include some security information in the manuals of the smartphones to enable customers read before using these devices. Also, students should handle their smart phones with care. Finally, a training programme should be design to equip the tertiary students to manage the threat efficiently

References

[1] Anzai, Y., Funada, M., & Akahori. K. (2013). Immediate effects of mobile photo note-taking in English vocabulary learning. *In T. Bastiaens & G. Marks (Eds.), Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, pp. 550-556).* Chesapeake, VA: AACE. Retrieved June, 2019 from http://www.editlib.org/p/114891.

[2] Buskirk, T. D. & Andrus, C. (2014) Smart surveys for smartphones: Exploring various approaches for conducing online mobile surveys via smartphones. *Survey Practice*, 5. (2012). Retrieved July, 2019 from http://36.22.354a.static.theplanet.com/ index.php/ Survey Practice/article/view/63.

[3] Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy in, Proceedings of the Eighth Symposium on Usable Privacy and Security, ser. *SOUPS '12. New York, NY, USA: ACM, p. 1:11:16.*

[4] Jones, B. H., & Heinrichs, L. (2012). Do business students practice smartphone security, *Journal of Computer Information Systems*, vol. 53, no. 2, pp. 22–30.

[5] Kambourakis, G. (2013). Security and Privacy in m-Learning and Beyond: Challenges and Stateof- the-art. *International Journal of u- and e- Service, Science and Technology*. 6(3), pp.67-84.

[6] Kissel, R. (2013). Glossary of key information security terms. *National Institute of Standards and Technology, Tech. Rep. NISTIR 7298 Revision 2.*

[7] Landman, M. (2010). Managing smart phone security risks. *Information Security Curriculum Development Conference*, ser. InfoSecCD '10. New York, NY, USA: ACM, p. 145155.

[8] Mansfield-Devine, S. (2012). Paranoid android: just how insecure is the most popular mobile platform? *Network Security, vol. 9, pp. 5–10.*

[9] Mylonas, A. Kastania, & Gritzalis, D. (2013). Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security*, vol. 34, pp. 47–66.

[10] Norries, C., Hossain, A., & Soloway. E. (2011). Using smartphones as essential tools for learning: A call to place schools on the right side of the 21st century. *Educational Technology, 51(3), 18-25.*

[11] Osang, B. F., Ngole. J., & Tsuma. C. (2013). Prospects and Challenges of Mobile Learning Implementation in Nigeria: Case Study National Open University of Nigeria (noun). *A paper presented at International Conference on ICT for Africa 2013, February 20 -23, Harare, Zimbabwe.*

[12] Panko, R. (2009). *Corporate Computer and Network Security*, 2nd ed. Boston: Prentice Hall.

[13] Urban, J. M., Hoofnagle, C. J., & Li, S. (2012). Mobile phones and privacy. *Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2103405.*

[14] Woodcock, B., Middleton, A., & Nortcliffe, A. (2012). Considering the smartphone learner: An investigation into student interest in the use of personal technology to enhance their learning. *Student Engagement and Experience Journal, 1(1), 1-15.*