RESEARCH ARTICLE

European Journal of Education and Pedagogy
www.ej-edu.org

Assessing Mobile Device Security Awareness Among First-Year Undergraduate Students in Ghana: The Case of The University of Cape Coast

John K. E. Edumadze, Alexander N. T. Kissiedu, Stephen E. Mensah, and Benedict A. Biney

ABSTRACT

The mode of teaching and learning has seen major changes since the inception of COVID-19. Some institutions apply technology to integrate face-to-face teaching approaches with online learning systems or wholly teach some of their courses online. Mobile devices, therefore, play a significant role in promoting teaching and learning. The increasing use of these devices comes along with several vulnerabilities that have the internet as its major source. The question to ask is, are students security conscious about or aware of these mobile security threats? Hence the intention is to assess mobile device security awareness among students at the University of Cape Coast, Ghana. A descriptive design was used for the study. A total of 1600 first-year undergraduate students were selected for the study. The study revealed that most students have little knowledge of mobile device security such as not-knowing their serial number, IMEI, data encryption, or activated SIM card PIN and their behaviour towards mobile devices which included making their Bluetooth visible, connecting to any Wi-Fi so far as they would get internet connectivity, downloading applications and files on the internet without being protected, makes most vulnerable and exposes them to a higher risk of being hacked and invaded by intruders.

Keywords: biometrics, awareness, mobile devices, security, threats, vulnerabilities.

Published Online: December 30, 2022

ISSN: 2736-4534

DOI: 10.24018/ejedu.2022.3.6.503

J. K. E. Edumadze
Network & Infrastructure Section,
UCC, Cape Coast, Ghana
(e-mail: jedumaze@ucc.edu.gh)
A. N. T. Kissiedu *
IT Training & Support Section,
UCC, Cape Coast, Ghana
(e-mail: alexander.kissiedu@ucc.edu.gh)
S. E. Mensah
IT Training & Support Section,
UCC, Cape Coast, Ghana
(e-mail: stephen.mensah@stu.ucc.edu.gh)
Stephen.mensah@stu.ucc.edu.gh)
B. A. Biney
IT Training & Support Section,
UCC, Cape Coast, Ghana
(e-mail: benedict.Biney@ucc.edu.gh)

****Corresponding Author***

I. Introduction

The covid-19 pandemic has had a major effect on educational systems globally. The President of the Republic of Ghana ordered the closure of all educational institutions in Ghana, affecting over half a million tertiary education students (UN Ghana, 2020). Similar decisions were taken by other countries or local authorities around the world to curtail the spread of the disease (UNESCO, 2020). Heads of academic institutions, including the University of Cape Coast, had to adopt various electronic learning technologies, either asynchronous or synchronous were adopted to keep learners busy. The YouTube distribution of pre-recorded lecture films enabled the asynchronous component of the training, allowing students to learn at their own pace; whereas the synchronous element of the teaching was carried out using video conferencing platforms such as Microsoft Teams, Zoom, and Google Meet (Lapitan Jr. *et. al*., 2021).

Regardless of the mode of assessing teaching and learning materials, students in tertiary institutions use mobile phones and other communication gadgets to facilitate learning. They send and receive messages, discuss class materials online, look up information, and databases in the library for educational resources, and hold group conversations with fellow students. Institutions with fewer internet connectivity tools encourage the 'bring your own device' (BYOD) policy to augment their resources.

The significant increase in the use of these mobile devices implies an increase in their vulnerabilities as well as a proportional rise in the exploits of these vulnerabilities. In the contemporary era, mobile devices are designed to provide broad Internet and network connectivity through varying channels such as cellular networks, Wi-Fi, and Bluetooth. Access points to such channels are all vulnerable to malicious attacks thereby compromising the key fundamental principles of confidentiality, integrity, and availability (Singh & Tiwari, 2015).

Abro (2018) asserts that vulnerabilities in mobile communication have been exploited since the inception of the first-generation mobile network (1G) through to the fourth generation (4G). The current fifth generation, 5G network is still in its early days. Mobile applications are injected with malicious codes by criminals so that can eavesdrop on calls and steal or damages data on the device. With the variety of communication mechanisms available and the increasing use of applications on mobile devices, the security threats to mobile devices have evolved to all the threats applicable to desktops or laptops, with additional threats that are truly unique to mobile devices. Therefore, people are to be aware of mobile device security and the need to be protected with an even broader set of security

techniques than those used for traditional desktop or laptop operating environments.

In recent times, newly admitted students at the University of Cape Coast are informed to report to campus with internet-ready mobile devices. For most of these students, owning such devices is a new experience because, at the Senior High School (SHS) level, students are not permitted to use any form of mobile device. How security conscious is a fresh undergraduate student who hitherto had not had any opportunity to use a smartphone in an academic setting for the first time without any restrictions? Hence this study aims to assess mobile device security awareness among first-year undergraduate students at the University of Cape Coast, Ghana.

A. Study Objectives

The following objectives guided the study:

1) Investigating various forms of device security used by students.
2) Assessing the relationship between mobile phone theft and basic device security awareness and implementation.

II. Literature Review

Smartphone usage has become so varied that it would be near impossible to document every available usage of the mobile phone. Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe (Ruggiero & Foote 2011). Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker. Malicious software can also send device information to attackers and perform other harmful commands. Mobile phones can also spread viruses to PCs that they are connected to. According to MOVR (2017), smartphones are the most used mobile device in the world, where it was revealed that South America, Africa, and Oceania recorded 91%, 79%, and 79% respectively use smartphones. Mobile phone usage in Ghana has increased sharply between January 2020 to January 2021 by 3.1 million from 41.69 million (Kemp 2021). A study by Moletsane and Tsibolane (2021) among students in higher education in South Africa revealed that smartphones were the dominant device owned by participants, followed by laptops, and then tablets.

Furthermore, Google Android turned out to be the most used OS, followed by Apple iOS before Windows OS. Google Play Store provides millions of mobile applications for Android OS users and therefore provides a haven for malicious attacks. McAfee reported in their first quarter report for 2018 that malware and other related attacks in the Google Play Store shot up by 30% over what was recorded in 2016.

Security is about data protection, but a more comprehensive security solution relies on strong encryption to keep assets safe from prying eyes. To Sujithra and Padmavathi (2012), some mobile device security challenges include poor authorization and authentication but relying on device identifiers such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), universally unique identifier (UUID) values for security is a recipe for a failure and can lead to broken authentication and privilege access issues. Therefore, performing advanced encryption would protect the user from being hacked or breached. Ironically, many organizations are reluctant to deploy strong encryption technology, such as Advanced Encryption Standard (AES) because it can significantly drag down device performance (Intel Corporation, 2013). Awareness of unique identifiers such as International Mobile Equipment Identity (IMEI) number may to an extent help track mobile devices though (Hooi *et al*., 2018; Sharma, 2021). The primary function of an IMEI number is to identify a mobile device. Manufacturers and telecom service providers exchange IMEI numbers to facilitate the tracking of mobile devices that could be stolen or unlawfully compromised. The IMEI of active mobile numbers in the network is recorded by the Equipment Identity Registry. The IMEI can also be used to confirm if a call originated from a certain phone or not. According to Kao (2011) in case a mobile phone is stolen or gets lost, the IMEI number is required for registering a complaint at the Police station and may help in tracking the mobile phone through the service provider. However, the mobile device's IMEI can be readily modified to mimic another person. For instance, it would be challenging to identify the true owner of the mobile device if someone with bad intentions obtained the IMEI number of a discarded mobile device and used it on another mobile device. These returned IMEI numbers can also be utilized to get around the blacklist of IMEIs for stolen mobile devices. Additionally, someone can have simple access to the apps that use the IMEI as an identification number if the IMEI number is hacked (Sharma, 2021).

According to Ruggiero and Foote (2011), losing a mobile phone used to mean only losing contact information, call histories, text messages, and possibly photos; however, in recent years, losing a smartphone has also put financial information stored on the device in banking and payment apps, as well as usernames and passwords used to access apps and online services, at risk. The value of the stolen equipment does not make up a big chunk of the total price tag. The things that cost the most are the intellectual property value of the devices, the fines for data breaches, and the legal requirements for notifications. When a mobile device is lost or stolen, it can be expensive for both the owner and the business. If the phone is stolen, attackers could use this information to access the user's bank account or credit card account. An attacker could also steal, publicly reveal, or sell any personal information extracted from the device, including the user's information, information about contacts, and GPS locations. Users may not always know about or be willing to use the many ways to protect their mobile devices from being lost or stolen (Tu & Yuan, 2012). A balance may need to be found between how much security countermeasures cost, how well they work, and how easy they are to use. It is also important to know how users react to security problems. But most mobile devices are owned or maintained by the user, not the company. Because of this, companies usually leave it up to end users to protect mobile devices, which can be risky because a security breach could cost a lot of money. Practitioners have

paid a lot of attention to the risk of losing or having a mobile device stolen, but as far as we know, no academic study has been done on this subject yet. Existing studies of security behaviour are usually done in the context of enterprise information systems, where businesses try to get their employees to keep company secrets safe.

Because most mobile devices now have Internet access, common web-based threats that have infected laptops or desktops may also affect mobile devices. A device connected via Wi-Fi or Bluetooth is more vulnerable because the Wi-Fi source or another Bluetooth-enabled device may have been compromised and is therefore vulnerable to other attacks. Users may connect to a rogue network access point that an attacker has deployed. The attacker may then intercept user communications to launch other attacks like phishing (Hogben & Dekker, 2010).

The depth of knowledge of mobile device security of university students who were digital natives was the focus of a study by Gkioulos *et al*. (2017). One of the studied topics for awareness is network access and the use of unprotected, open Wi-Fi networks. By sniffing, spoofing, or eavesdropping, attackers can corrupt, obstruct, or change information on the wireless network (Jeon *et al*., 2011). Other security issues with mobile device use were noted by Sujithra (2012), including the storage of sensitive data without any security or encryption. Additionally, if applications base security decisions on user input, malware or client-side injection attacks may take advantage of this to use paid resources, get access to private data, and escalate privileges.

Sujithra (2012) classified mobile device threats into four categories: physical, web-based, network-based, and application-based threats. Physical catastrophes or vandalism, gadget theft, and Bluetooth attacks are examples of physical attacks. A user may become vulnerable to assaults such as phishing scams, browser exploits, and unauthorized downloads when using the internet and other web services. Network exploits, wi-fi sniffers, and the use of mobile network services like SMS or voice calls as attack vectors are some examples of network-based threats.

Applications' flaws give the necessary ground for an assault. Most users trust platform owners and assume the programs they download from repositories are secure because they lack awareness of, and knowledge of the security measures platform owners take to assure the security of the applications offered in their application store. Because viruses can pretend to be helpful programs (Mylonas *et al*., 2013; Ophoff & Robinson, 2014), this can be a serious vulnerability.

III. Methodology

A. Participants

The study population comprised about 5600 freshly admitted undergraduate students for the 2020/2021 academic year. Random sampling was used to obtain the sample size of 1600 respondents for the study at the University of Cape Coast ICT Centre.

B. Research Design

A cross-sectional survey design was espoused. A quantitative research design was adopted, and the study was conducted only at the University of Cape Coast, Ghana.

C. Instrument

Google form was used to design structured questionnaires that were administered to the respondents via the Institution's electronic learning platform. The survey comprised questions in relation to freshly admitted students' mobile device usage, and security awareness.

IV. Results and Discussion

A. Demographic Characteristics of the Respondents

The demographic data of the population are presented in Table I. The number of male respondents was higher than the females with a percentage of 58% as against 42%. It was also observed that 4.2% of the respondents were less than 18 years, 93.1% were between 18–24 years, 2.3% were between 25–34 years, and 0.3% were between 35–44 years. One of the respondents was over 44 years whereas two of the respondents declined to indicate their age. The data suggest that most people entering the University are aged between 18–24 years and are therefore mature enough to take their own decisions.

TABLE I: Sex, and Age of Respondents

		Frequency	Percent
Sex			
	Female	672	42.0
	Male	928	58.0
	Total	1600	100.0
Age			
	<18	67	4.2
	18–24	1489	93.1
	25–34	37	2.3
	35–44	4	0.3
	>44	1	0.1
	Decline	2	0.1
	Total	1600	100.0

B. Assessing the Form of Mobile Devices' Basic Security Features

To have a clearer understanding of mobile device security being used by the respondents, the number of mobile phones and the type of mobile devices used were assessed.

TABLE II: Number of Phones Used by Undergraduate Students

Number of phones	Frequency	Percent
One Phone	1332	83.3
Two Phones	225	14.1
More than two phones	43	2.7
Total	1600	100

It is evident from Table II that all undergraduate students owned at least a mobile. Most of them (83.3%) had a phone, 14.1% had two phones, and 2.7% had more than two phones. This agrees with a mobile statistics report by

Radicati (2014) where most of the respondents (83.9%) had just a phone, 12.8% of the respondents were using two phones, and 3.1% of respondents were using more than two phones.

Fig. 1 is a display of mobile devices owned or used by the students. Smartphones are the predominantly used mobile devices, with the least being tablets. It can be deduced that most undergraduate students enter the university without a notebook/laptop. This finding is in line with that of MOVR (2017). They found that 93.9% were smartphone users, 5.9% were tablet users, 0.4% were Notebook users, 13.9% were Laptops, and 7.1% were using feature phones (none-smartphone).

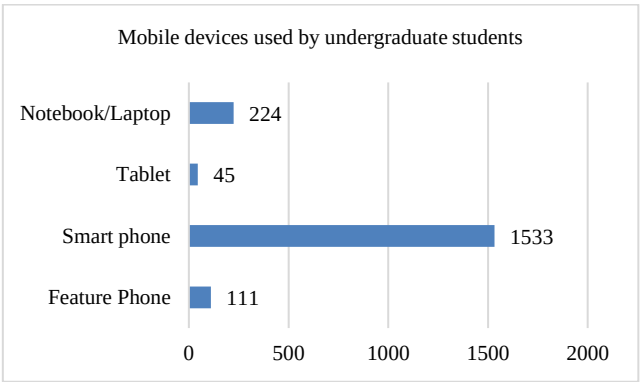

Fig. 1. Mobile devices owned by undergraduate students.

Fig. 2 is a display of the various operating systems (OS) installed on the various mobile devices of the respondents. Android is the most popular OS in use. This could perhaps be due to the popularity of android mobile devices largely because they are relatively cheaper. Less than 100 students claimed they have devices that use Apple iOS, However, 87, students did not know about the OS they have on their devices. This is in contrast with a study by Harris *et al.* (2015) who asked respondents to specify the operating system they used on their main smartphone, tablet, or both. It was discovered that Apple's iOS was used by 60.8% more people than Google's Android, which was used by 43.5%. A little proportion of respondents, 4.3%, said they used both iOS and Android, and 3.3% of respondents use operating systems other than Google and Apple operating systems.

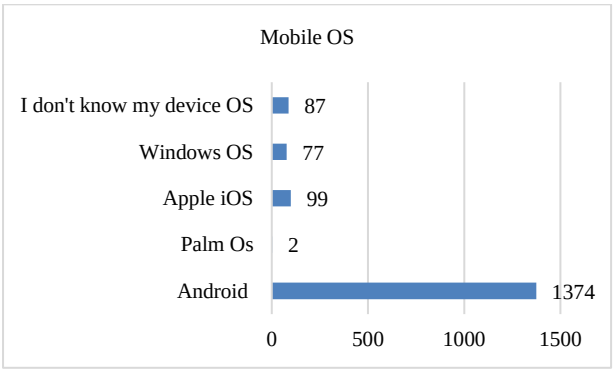

Fig. 2. Mobile operating system used by undergraduate students.

C. Exploring the Association between Mobile Phone Theft Experience and Awareness of Basic Security and Its Implementation

TABLE III: DISTRIBUTION OF PHONE THEFT EXPERIENCE AND BASIC PHONE SECURITY AWARENESS

	Frequency	Percent
Has your phone been stolen before?		
Yes	529	33.1
No	1070	66.9
Have you activated your Sim card PIN?		
Yes	572	35.8
No	783	48.9
I don't know the Sim card PIN	245	15.3
Have you noted your IMEI number?		
Yes	412	25.8
No	742	46.4
I don't know about the IMEI number	446	27.9
Have you noted your serial number?		
Yes	345	21.6
No	935	58.4
I don't know about Serial number	320	20.0
Are you familiar with data encryption?		
Yes	542	33.9
No	741	46.3
I don't know about Serial number	317	27.9

Undergraduate students' responses to their level of awareness of features such as Sim card PIN activation, data encryption familiarity, and whether they have noted IMEI number, or the serial number of their mobile device followed a similar trend. In all cases majority of them said they have not activated their Sim card PIN, are not familiar with the data encryption features of their mobile device, have not noted their IMEI number, nor have they taken notice of the serial number of their device. It can be inferred from Table III that for all the issues examined, those who have activated their Sim card PIN, noted their IMEI and the serial number of their devices, and are familiar with the data encryption features of their devices are more than those who are not.

Even though knowledge of identifiers such as IMEI and serial numbers may not be a good security option, they can, to an appreciable degree, help in uniquely identifying devices. Suithra and Paddmavathi (2012) are advocates of advanced encryption. According to Ruggiero and Foote (2011) when choosing a mobile phone, the user is expected to consider its security features such as file encryption, the ability to wipe the device or delete known malicious apps remotely, and authentication features. But as indicated in Table III, more than 50% of the respondents neither know about data encryption nor are familiar with it.

Some people have had their data stolen or confidentiality breached after having had their mobile phones stolen or losing them. Table III indicates that 66.9% of the respondents have never lost their mobile device, and 23.1% have lost their device at least once. Since most of the respondents are not familiar with basic security features such as Serial numbers and the encryption functionality of their devices, they risk losing very important data.

To further explore the association between those who have had their mobile phones stolen or not and the notice of

basic security features, the following hypotheses were formulated:

H1: There is no significant association between mobile phone theft experience and sim card activation.

H2: There is no significant association between mobile phone theft experience and IMEI number notification.

H3: There is no significant association between mobile phone theft experience and serial number notification.

H4: There is no significant association between mobile phone theft experience and data encryption familiarity.

For all the relationships explored, sim card activation (χ^2 =3.623, df=2, ρ=0.163), IMEI number notification (χ^2 =4.284, df=2, ρ=0.117), serial number notification (χ^2 =1.927, df=2, ρ=0.382), and encryption familiarity (χ^2 =0.637, df=2, ρ=0.727) did not have any significant relationship with mobile phone theft experience.

The results presuppose that undergraduate students may not necessarily activate their sim card activation or take notice of their IMEI number. They would also not be bothered about the data encryption feature on their device. A probable reason for this trend could be that most students entering university from senior high school may be using smartphones for the first time and do not lose much when their devices are stolen.

D. Mobile Connectivity Risk Awareness

Mobile device network connectivity has often been the gateway to hacking and unwarranted intrusion. in this regard, respondents' views were solicited about how they connect to other networks. Results presented in Table III indicate that most respondents are not aware of the security threats they are exposing themselves to by casually handling their Bluetooth or Wi-Fi connectivity options. Most of them (77.6%) usually leave their Bluetooth switched on and visible, 13% have their Bluetooth switched off, 5.9% turn them on but are invisible, and 2.2% do not know the difference between their Bluetooth device being visible and invisible. When it comes to Wi-fi connectivity, 64.9% of the respondents are oblivious to the risks associated with such connections so long as they can access the internet, and 33.8% said they only restrict themselves to secure Wi-fi.

In responding to their awareness of the availability and use of antivirus specifically for mobile phones, 37.3% of the respondents confirmed they use it, a similar percentage (35.4%) do not use it although they knew about it, 23% of them did not know about the existence of antivirus for mobile phones. Thus, it would be easy for respondents to contact viruses via copying and downloading applications, videos, and files that breach their security for intruders.

E. Risk of Exposing or Losing Sensitive Data

How respondents manage their information on their devices, and whether they back-up such information was examined. Their responses have been presented in Table IV. On the issue of whether sensitive personal data such as photos and videos are kept on mobile devices, 72.8% responded positively to keeping such items on their devices as against 27.3% who do not keep such data on their devices.

The study also revealed that 60.2% of the respondents do not store their passwords or PINs on their phones, 20.7% save those credentials in an encrypted phone, and 19.1% save them without encrypting them. Despite the storage of sensitive data on their devices, 36.1% said they do not often back up, 24.2% have never backed up, and the rest back up at least 2–3 times per month. As Sujithra and Padmavathi (2012) put it, storing sensitive data on a device without any form of encryption or protection may lead to lead to exposure of sensitive information.

TABLE III: USER BLUETOOTH AND WI-FI CONNECTIVITY BEHAVIOR

	Frequency	Percent
Bluetooth connectivity user behaviour		
I don't know the difference between visible and invisible	35	2.2
My phone doesn't have Bluetooth	7	0.4
Switched off	221	13.8
Switched on and invisible	95	5.9
Switched on and visible	1242	77.6
Wi-Fi connectivity user behaviour		
I don't care about the source so long as I can access it	1038	64.9
I only restrict myself to secure Wi-Fi (Password required)	540	33.8
My phone doesn't have a Wi-Fi feature	22	1.4
Antivirus for mobile phones		
I don't know if there is such a product for my phone	381	23.8
I know there is, but I don't use it	566	35.4
My phone doesn't have the ability	57	3.6
Yes	596	37.3

TABLE IV: STORAGE OF SENSITIVE INFORMATION AND BACKUP CREATION

	Frequency	Percent
Do you keep sensitive personal data on your phone (photos/videos/discussion recordings)?		
No	436	27.3
Yes	1164	72.8
Do you store important passwords and PINs on your phone?		
No	963	60.2
Yes and "encrypted"	331	20.7
Yes, without encryption	306	19.1
How often do you create backup copies of your device data?		
2-3 times per month	141	8.8
Less often	577	36.1
More than 3 times per month	142	8.9
Never	387	24.2
Once per month	353	22.1

F. Awareness Of Biometric Features and Choice of Biometric Protection Features

Biometric features on mobile devices ensure privacy in data protection. Respondents were asked whether their devices supported biometric protection and whether they had them enabled. Their responses have been captured in Table V. It can be observed that a greater percentage (57.5%) had devices that did not support biometric protection, 26.1% had biometric-ready devices, and 16.4% could not tell whether their devices had such features. Out of the number that had devices with biometric features, 71.3% have the features enabled and 28.7% not having enabled them.

G. Biometric Protection Feature Preference

Fig. 3 indicates respondents' biometric preferences. Most of the respondents indicated that they would prefer using a fingerprint scan, with a similar number (127) preferring either voice recognition or iris recognition. A plausible reason for their overwhelming choice of fingerprint scan is its popularity as a security feature in most electronic devices.

TABLE V: BIOMETRIC FEATURES AND CHOICE OF BIOMETRIC PROTECTION

	Frequency	Percent
Does your device support biometric protection features?		
I don't know	263	16.4
No	920	57.5
Yes	417	26.1
If yes, have you enabled biometric protection?		
No	138	28.7
Yes	343	71.3

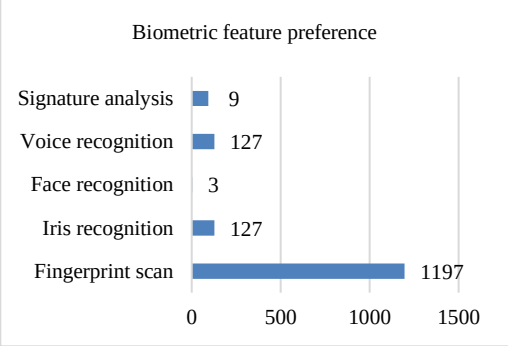

Fig. 3. Respondents' biometric feature preference.

V. CONCLUSION

The undergraduate students entering the University of Cape Coast have at least one mobile device which could be a feature phone, tablet, smartphone, or laptop. This notwithstanding, they are oblivious of security threats such as virus attacks and hacking. They fail to take basic security measures such as taking notice of the serial numbers of their mobile devices and exploring their security features. They opt to connect to any available Wi-fi network just for internet access or leave their Bluetooth on and visible without considering virus attacks or electronic frauds, data breaches, and viruses that they may be affected with through their activities. However, it was seen that they save most of their valuable items such as passwords, sensitive information, and lifetime experience on their mobile devices. When given the opportunity, most students would prefer to have a finger scan biometric protection feature on their mobile devices to safeguard their valuable items on their mobile devices.

VI. RECOMMENDATION

The following recommendations were made based on the findings.

1) University authorities should include mobile security awareness in the orientation program for newly admitted undergraduate students.
2) There is a need for mass education on the risks of saving sensitive information on mobile devices.

The study was conducted on one tertiary institution in Ghana, thus future studies should look at mobile security awareness in more than one tertiary institution to gather more evidence based on mobile security awareness.

REFERENCE

Abro, A. B. (2018). Mobile networks security landscape. In M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, & M. Ylianttila (Eds.). *A comprehensive guide to 5G security*. (pp. 59–74). John Wiley & Sons. https://www.researchgate.net/publication/316244138_A_Comprehensive_Guide_to_5G_Security.

Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information*, 8(2), 42.

Harris, M. A., Chin, A. G., & Brookshire, R. (2015). Mobile app installation: the role of precautions and desensitization. *Journal of International Technology and Information Management*, 24(4), 3.

Hogben, G., & Dekker, M. (2012). *Smartphones: Information security risks, opportunities and recommendations for users/European Network and information Security Agency (ENISA) – Forschungsbericht*.

Hooi, Y. K., Kalid, K. S., & Tachmammedov, S. (2018). Multi-factor attendance authentication system. *International Journal of Software Engineering and Computer Systems*, 4(2), 62–79. https://journal.ump.edu.my/ijsecs/article/view/705/143.

Intel Corporation (2013). Strong Mobile Device Security Begins in the Hardware. Printed in USA 1113/PC/PRW/PDF Please Recycle 329623-001US. https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/enterprise-security-mobile-device-windows-8-1-brief.pdf.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011, July). A practical analysis of smartphone security. In Symposium on Human Interface (pp. 311–320). Springer, Berlin, Heidelberg. https://link.springer.com/content/pdf/10.1007/978-3-642-21793-7_35.pdf.

Kao, I. L. (2011). *Securing mobile devices in the business environment*. IBM Global Technology Services–Thought Leadership White Paper.

Kemp, S. (2021, February 11). *Digital in Ghana: all the statistics you need in 2021-datareportal-global digital insights*. Data Reportal-Global Digital Insights, Data Reportal-Global Digital Insights. https://datareportal.com/reports/digital-2021-ghana

Lapitan Jr, L. D., Tiangco, C. E., Sumalinog, D. A. G., Sabarillo, N. S., & Diaz, J. M. (2021). An effective blended online teaching and learning strategy during the COVID-19 pandemic. *Education for Chemical Engineers*, 35, 116–131.

McAfee, (2018). *McAfee Mobile Treat Report Q1, 2018, McAfee*. Santa Clara, CA, USA. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf.

Moletsane, T., & Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. *In 2020 conference on information communications technology and society (ICTAS)* (pp. 1–6). IEEE.

MOVR (2017). *Mobile overview report*. https://skydeo.com/wp-content/uploads/2017/11/Device-Map-Report-WURFL.pdf.

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

Ophoff, J., & 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.

Radicati, S. (2014). *Mobile statistics report, 2014–2018*. Palo Alto, CA: Radicati Group. https://www.radicati.com/wp/wp-content/uploads/2014/01/Mobile-Statistics-Report-2014-2018-Executive-Summary.pdf

Ruggiero, P., & Foote, J. (2011). Cyber threats to mobile phones: carnegie mellon university. Produced for US-CERT, a government organization. https://www.cisa.gov/uscert/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Sharma, R. (2021). Analysis of security risks associated with imeis and unwiped data of disposed mobile handsets. *International Research Journal of Modernization in Engineering Technology and Science*, 3(11),659–662. https://www.irjmets.com/uploadedfiles/paper/volume_3/issue_11_november_2021/17180/final/fin_irjmets1637305506.pdf

Singh, R. K., & Tiwari, N. (2015). An investigation on wireless mobile network and wireless lan (wi-fi) for performance evaluation. *International Journal of Computer Applications*, 126(6). 1–8. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=58f6ce34c31f81e72aac852e34b62c4535fd0044

Sujithra, M. & Padmavathi, G. (2012). Mobile device security: a survey on mobile device threats, vulnerabilities, and their defensive mechanism. International Journal of Computer Applications, 56(14), 24–29. https://doi.org/10.5120/8960-3163.

UNESCO, (2020). *Half of world's student population not attending school: UNESCO launches global coalition to accelerate deployment of remote learning solutions*. https://en.unesco.org/news/half-worlds-student-population-not-attending-school-unesco-launches-global-coalition-accelerate.

United Nations, Ghana (2020). *COVID-19: Impact on Ghana's Education*. https://ghana.un.org/en/45322-covid-19-impact-ghanas-education.