Assessment of Security Awareness Level of Mobile Device Users in Tertiary Institutions in Plateau State of Nigeria

Abayomi Jegede[1], Grace Odii[1], Musa Magaji[1], and Gilbert Aimufua[2]
[1]Department of Computer Science, University of Jos, Nigeria
Email: jegedea@unijos.edu.ng
[2]Department of Computer Science, Nasarawa State University, Keffi
Email: aimufuagio@yahoo.com

Abstract—Mobile devices are widely used in everyday life, however, the number of cyber-attacks on the security and privacy of mobile device users are increased. Although students at tertiary institutions are savvy Internet users, there appears to be a gap between their behaviors and the security of their mobile devices. The security awareness of mobile device users in tertiary institutions in Nigeria's Plateau State is assessed in this article. The study looks into mobile security vulnerabilities, as well as whether or not users are aware of them and what tactics (if any) they take to deal with them. A questionnaire is used as an instrument to acquire information about consumers' security awareness. The purpose is to see if academic literacy and the ability to utilize mobile devices are related to security awareness and the implementation of relevant security measures. It also tries to figure out whether users who value mobile device security and have legitimate security concerns engage in behaviors that either enhance or compromise security. The findings demonstrate that the majority of students (58.4%) have a strong understanding of their devices (including their functions) and that a substantial percentage of students (85.6%) regard mobile device security to be vital. Furthermore, (63.4 %) of respondents are concerned about the security of their mobile devices. In conclusion, the outcome of this study shows that smartphone users have little knowledge of security and privacy on smartphones but then the level of security awareness using smartphones is increasing as respondents answered the questionnaire.

Index Terms—mobile device, privacy, probability sample, smartphone, security awareness.

I. Introduction

A MOBILE device is small-sized computer or telephone that is held and operated in the hand. These devices consist of a touchscreen interface with a digital buttons and keyboard. Modern mobile devices use Bluetooth, near field communication (NFC), cellular networks and Wi-Fi technologies to connect to the Internet and interconnected with other devices. The devices possess in-built cameras which support voice and video calls. They also support video games and provides their owners with geolocation services using the Global Positioning System (GPS). Mobile devices usually run a mobile operating system, which provides platform to execute proprietary and third-party applications. These applications come in small-sized, low scaled versions specially built to suit the small memory size and low processing power of mobile devices. Hence, they are called mobile applications or mobile apps for short. Mobile devices have become increasingly popular among a wide range of users due to their small size, light weight and ease with which they can be carried around. Other major appeals of mobile devices include their ubiquitous capabilities and support for a wide range of application such as phone calls, email, mobile or Internet banking, electronic commerce, online meetings among others. This makes it easier for people to carry out their daily tasks on the go and without the need of a computer or physical office locations. Mobile device is an important and widely used tool in daily activities and virtually in all sectors of the economy. This is because mobile devices provide easy communication, faster and seamless business operations and better productivity for individuals and teams within organizations. Currently, the global ownership of smartphones is about 6.378 billion people, which represents 80.76% of the people in the world [1]. It is estimated that nearly 75% of the global population will access the Internet exclusively via their smartphones by 2025 [2]. The number of mobile Internet users in Nigeria stands at 101.72 million, with the figure rising steadily from 39.57 million in 2016 to 101.72 million in 2021, with a projected rise to 142.73 million in 2026 [3]. Apart from the increasingly large ownership of mobile devices, large amounts of vital and sensitive personal information are increasingly stored, processed and transmitted by mobile devices. Organizations deploy mobile applications to achieve competitive business edge, while customers can easily download and use mobile apps to access the services provided by business enterprises. Manufacturers release new and exciting mobile devices into the market regularly to provide enhance features and capabilities over the previous version. The global disposable income has increased over the years, which enable more people to acquire mobile gadgets. These developments have attracted the interest of hackers who regularly develop and deploy various malicious tools and techniques to exploit mobile devices and applications. Common attacks against mobile devices include malware (virus, worm, Trojan horse, ransomware, spyware, adware), password cracking, spoofing, and side-channeled attacks. Cyber threats against mobile devices in Nigeria rose to 35% in 2018 and has been on the rise since then [4]. This makes the security of mobile devices (as well as the information stored in them) very important. Security of data and information is a major concern in implementing mobile and wireless solutions. This is quite challenging because it is more difficult to protect personal and enterprise data in wireless transmission and mobile storage than in a wired environment. The sensitivity of data and information in mobile devices place a huge responsibility on users of such devices to ensure the confidentiality, integrity, and availability of their devices and

the information stored in them, from those with malicious intentions. Majority of mobile device users place much emphasis on features and functionalities of devices, with little or no concern for the security of those devices and protection of information stored in them. Manufacturers of mobile gadgets advertise their products based on the features of those devices and the functions they perform. They make very little or no mention of the security features and capabilities of their products.

Mobile device security awareness is the knowledge or perception about and attitude towards the protection of actual physical gadgets as well as information stored in them. It is the concern about and well-informed interest in the physical and logical security of mobile devices. Lack of adequate security awareness constitutes a major to the security and protection of mobile devices. It has been established that humans are weakest link in the information security or data protection chain. Attackers are able to exploit systems and networks mainly due to ignorance or negligence of humans who manage or use information systems. Low level of security awareness cut across a wide range of users irrespective of social, economic or educational background. Many people simply buy phones, install favorite application and start using the device, without providing basic security measures such as personal identification number (PIN), password, screen protection or antivirus. Students of tertiary institution are among the most computer literate members of every society [5]. They also constitute a major group of users of mobile devices. It is often assumed that they are aware of the threats that confront mobile device and Internet users. However, studies have shown that the reverse is the case [5,6]. A lot of mobile device users are not adequately informed about security issues associated with the use of mobile gadgets. Most of the users who are aware of security threats fail to adopt proper security measures and practices. The increasing popularity of mobile devices and their use for storing large amounts of sensitive personal, financial and commercial information attract both targeted and large-scale attacks. It is quite challenging for information officers and cyber security professionals to provide device security, data protection and reliability at the frontlines.

Several studies have been carried out to evaluate the security awareness of mobile device users [7,8,9,10,11,12]. However, none or few of these studies explored mobile security awareness specifically among students of the tertiary institutions. To the best of our knowledge, this is the first study that focused on cyber security awareness of mobile device users in tertiary institutions in Nigeria. A major contribution of this study is that it will demystify the erroneous belief that students of tertiary institutions are information technology savvy and are aware of the security risks and threats associated with the use with the used of mobile gadgets. It eliminates the assumptions that the level of literacy of these category of users guarantees that they adopt proper security measures and practice. This study provides baseline for similar studies in other parts of the country.

II. Related Work

Khan et al [7] presented various security challenges including threats and vulnerabilities faced by mobile ecosystem. The study emphasized secured programming or security (conscious development) and secured or safe application download as ways to ensure security of mobile devices. Other strategies proposed by the authors include security of mobile operating systems, in-built restrictions in mobile devices that prevent intentional or accidental installation of malicious application applications and the use of mobile devices. A study aimed at assessing the mobile security awareness of public sector employees involved a sample field survey of 120 workers who used mobile devices to carry out official tasks [8]. The questionnaires focused on issued related to the operating systems installed in the users' (employees) devices, physical access restriction strategies adopted by the respondents such as the use of screen lock whether the users use antivirus or anti-malware applications and whether application sources required access to device location or data prior to installation. Other questions focused on device sharing; that is, whether multiple workers use same mobile devices for official work and whether employees use their personal devices to access the organization's network. The study specified controls that be applied to the information Technology audit of the organization and provided recommendations for security mobile devices. A slightly different study used behavioral model theories evaluate the response of users to security features of smart mobile gadgets in the event of security breaches [9]. The survey focused on mobile hardware and software products preferred by users; behavioral tendencies of smart mobile device users as well as users' perception on mobile device security. The paper also proposed a novel framework based on the analysis and assessment of behavioral factors which influence a users' attitude to mobile device security. The findings from the research revealed that the widespread application of mobile devices in many aspects of the daily lives does not imply a satisfactory level of security awareness. The study also revealed that many mobile device users do not adopt basic security measures and are negligent of threats and vulnerabilities facing mobile devices. Users place personal satisfaction and ease of use far above security. Limited disposable income is also a challenge as many users consider the cost of security mechanisms such as antivirus much higher that any gain that could be made in terms of security and protection. They also consider regular update of antivirus (and other software) and the use of different password for different websites or applications a herculean task. The authors recommended that creating awareness on the implications of users' actions and behavior on the security of their mobile devices could result to in the overall increase in the level of security awareness of the users.

In an attempt to determine whether users understand the consequences of being a part of smart ecosystems. Kulyk et al [10] conducted a survey of 575 participants from Germany, Romania and Spain who use smart home and smart health applications and services. The study reported that almost half of the participants have at least one security and privacy concern. German participants are more concern about security and privacy than participants from Romania and Spain. The study shows that level of security and privacy awareness and consequently data protection regulations, their implementation and enforcement vary from country to country. This poses an enormous challenge if the goal is to achieve a global implementation of data protection regulations, their implementation of data protection regulations and enforcement considering the fact that Internet-based services extend beyond national boundaries. Smart home applications or services highlighted issues related to data collections without mentioning whether such data would be shared with third

parties. Although the users are aware of the sensitivity of the data provided to smart home and smart health applications, they seem not bothered about unauthorized sharing of data with third parties. This is because the user's trust in the operators of these applications or services or their agents. The study emphasized the relevance of cultural factors and operational environment of a specific system or data exchange to the security and privacy of the end users. A related study focused on business students who access online resources with the aid of mobile devices [11].

The goal was to investigate the attitudes, behaviors and practices of these category of students with respect to mobile device security. The students were divided into two groups. The first group consists of students who had no training on mobile security while a second group was made up of students who completed an online training program on mobile device security. The result revealed very little difference in the security practices of the two groups of students. This shows that online security training programs are largely ineffective in changing a user's security behavior and practices. This emphasized the need for further research on efficiency of training methods. A related work surveyed smartphone users to determined their level of security awareness and adherence to security behavior and practices [12]. The study explored privacy awareness level of smartphone users. The findings showed that many smartphone users have a very low level of security and privacy awareness. The major contribution of this study is the development of an easy-to-use method for assessing the 'level of awareness (LOA)' of smartphone users. Similarly, Rufai et al [13] applied quantitative online survey on 176 mobile device users to determine the cyber security awareness of the Nigerian public. The results showed that while moderate number of respondents are aware of the cyber security issues, majority of the users engage in bad practices such as weak passwords, usage of free anti-virus software, and password sharing. Many of the respondents (77.84%) are not aware of the existence of Nigeria Computer Emergency Response Team (ngCERT) as the body which manages and responds to cyber security risks, threats and breaches in Nigeria. The paper suggested that poor security practices of mobile device users is a major reason for the rapid increase in cyber-attacks in the country. Hence it is necessary for the country to improve its cybersecurity strategies and measures, including training of mobile device users and engaging in massive security awareness of smartphone users based on different parameters [14]. The authors divided the sample into different user groups based on demographic data and compare the level of security awareness of various user groups. Each user group has different age range, level of education, and IT security skills. The analysis revealed a fairly low level of security awareness among the respondents. It also showed that the oldest and the youngest groups of participants have the lowest level of security awareness. There is also a positive correlation between increasing level of security awareness and the level of education and IT security skills of the respondents.

III. Methodology

This study considered the general population of five tertiary institutions in Plateau State consisting of the University of Jos, Plateau State Polytechnic Barkin Ladi, College of Forestry Jos, College of Health Zawan, and NTA Television College Rayfield Jos. The sample for this research is a fraction of the population used for actual investigation. The Taro Yamane formulae was used to determine the sample size for the study. It is defined as $n = \frac{N}{1 + N(0.05)^2}$, where n is the desired sample size, N is the population size (total number of students of tertiary institution in Plateau state) and 0.05 is the level of significance of the percentage error for the ninety-five (95%) percent confidence interval. Although the actual population of students in the selected institutions is in excess of 50,000, but we could not determine the exact population size in the course of this study. Hence, we adopted an estimated population of 50,000 for this research. Therefore, the estimated sample n, for the study would be:

$$\begin{aligned} n &= N/ [1 + N (0.05) (0.05)] \\ &= 50{,}000/ [1 + 50{,}000(0.0025)] = 50{,}000/(1+ 125) \\ &= 50{,}000 /126 = 396.82539 \\ &\cong 397 \end{aligned}$$

Questionnaires were administered to 500 respondents instead of 397 in order to increase the coverage of sampling across the population. We used our knowledge and experience of what constitutes security awareness, security concerns and appropriate security practices to formulate the questions. The questions were tailored in such a way that responses obtained show whether the students have the necessary security knowledge (despite their high level of academic literacy and widespread use of mobile devices), whether they have concerns about device security and whether they practice behaviors that promote or compromise mobile device security. The technique used to gather data for the study is the simple random sampling which is also referred to as probability sampling. "Simple random sampling is a procedure in which the choice of a particular element does not jeopardize the chance of other element being selected into the same sample." [15]. This ensures that all units of the population have the same chance of being included in the sample. The respondents were randomly selected from five tertiary institutions, giving every respondent in the population equal opportunity of being selected. A total of 100 participants were females. The respondents consist of users between the age of 15-25 which amounts to 88.6% (443) of the total population. From the survey conducted, it was established that majority of the participant are indigenes of Plateau state, having a percentage of 71.2% (356). The instrument used to collect data for this research is questionnaire. The questionnaires were administered using local distribution (that is, face to face) technique. The data gathered was analyzed and summarized using tables and charts. The IBM and SPSS tool used allows for easy interpretation and analysis. The questionnaire was divided into two parts. The first part includes demographic data which includes institution name, gender, age, and place of residence. The second part covers specific questions related to security practices and perceptions by mobile device users. The goal is to determine whether the participants understand the security related features of their phones, their knowledge of mobile device security in general and whether they are taking the necessary measures to reduce the risks.

IV. Results and Discussion

This section presents the results of the analysis and discussion of findings made from the study.

A. Academic and Demographic Information

This section collects the academic and demographic information namely the institution, gender, age group and residents of the respondents of the students. Table 1 shows the demographic information of the respondents from each institution as well as the percentages.

The percentage of students from each of the five institution is 20%. This ensures that equal number of participants represents each institution. The participants from University of Jos, consist of 61% males and 39% Females. This shows that most of the participants are males. In Plateau State Polytechnic, 45% of the participant are males while 55% are females. This shows that there are more females respondents than the males. This is

TABLE I
DEMOGRAPHIC AND ACADEMIC INFORMATION

Institution	Frequency (%)	Gender (%)		Age (%)			Resident (%)	
		Male	Female	15-20	21-25	26-30	Yes	No
University of Jos	20	61	39	48	50	2	62	38
Plateau State Polytechnic	20	45	55	41	35	22	86	14
NTA Television College	20	36	64	46	44	9	57	43
College of Forestry	20	44	56	56	38	6	68	32
College of Health	20	44	56	42	43	7	83	17
Total	100	46	54	46.6	42	9.4	71.2	28.8

applicable to the other three institutions. The distribution of the sample consists of 46.0% (230) males and 54% (270) females. This shows that more females participate in the research. Females are considered to be more naïve when it comes to security and functionality of devices, but this survey shows that they are beginning to be conscious of mobile device security. Hence, both genders are considered to be at the same level as far as mobile device security is concerned. The table also shows that 46.6% (233) of the participants are between the ages of 15-20, while 42% (210) are between the ages of 21-25 years. This is because majority of students in tertiary institutions belong to this age group. In general, 63.6% (318) of participant live permanently in Plateau state, while 36.4% (182) does not. This shows that majority of the students in the tertiary institutions in Plateau State are resident in the state.

B. Mobile and Wireless User

The study assumed that almost all the users owned at least one device. One of the survey questions required a user to mention the type of mobile device he owns in order validate this assumption. Table 2 shows the types of devices owned by users in each institution and their distributions across the sample.

TABLE II
DEVICES OWNED BY USERS

Institution	Smart phones (%)	Tablet (%)
University of Jos	88	12
Plateau State Polytechnic	95	5
NTA Television College	90	10
College of Forestry	88	12
College of Health	89	11
Total	450 (90%)	50 (10%)

The result shows that majority of respondent (90% or 450) own smartphones. Smartphones are the most popular mobile devices among the students in these institutions. This is due to the fact that smart phones are portable, versatile and easier to use than tablets. The survey also showed that Android is the most widely used (75.6 % or 377) operating system among the respondents.

C. Personal and Application Security

The respondents were asked whether they use screen lock measures in order to determine their understanding of practices that enhance the security of mobile devices. The survey revealed that all the students use one or more screen protection measures ranging from password, PIN, pattern to fingerprint and antivirus. Fig. 1 presents the distribution of security measures used by the respondents.

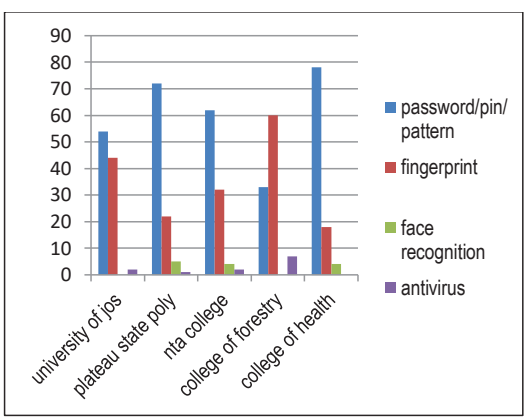

Fig. 1. Security measures.

Overall, 59.8% (299) 0f the respondents use password or PIN, 35.2 (176) use finger print and 2.4% (12) use antivirus on their mobile device. This prevents unauthorized persons from compromising the security of security of users or violating their privacy. The password screen lock alone is not sufficient to protect data against sophisticated attackers, but it is good enough in practice for most users as it mitigates the risk at the lowest level. Respondents from university of Jos, Polytechnic and Forestry (66%, 75%, and 64% respectively) tend to share their passwords and Automated Teller Machine (ATM) PIN

more than respondents from college of health and NTA college (26% and 42%). Table 3 shows that majority of the respondents (55.6% or 278) do not share their password or ATM PIN. This category of users is aware that PIN or password sharing exposes them to security risks. Fig. 2 shows the frequency with which respondents share their ATM PIN and passwords. More than half of the users do not share their passwords at all. A significant number (176 or 35.2%) rarely share their password as shown in Fig. 2. Without security measure and controls in place, users' data particularly in mobile devices might be subjected to an attack. These days, almost all mobile device users tend to keep sensitive personal data into their mobile devices for example like photos, videos, important document and discussion recordings to prove this hypothesis, we came up with this question: "Do you store credentials for financial applications and bank details in your mobile devices?"

The result in Table 3 shows that 62.2% (311) of the respondents tend to keep sensitive information on their mobile devices, while 37.8% do not. Although, this is not wrong practice, it is advisable from a security perspective. Access to mobile by unauthorized person exposes legitimate owners of such device to unquantifiable risks. Hence, owners of mobile devices should apply appropriate security measures on their devices and information stored in them in order to mitigate the risks associated with loss of compromise of such devices.

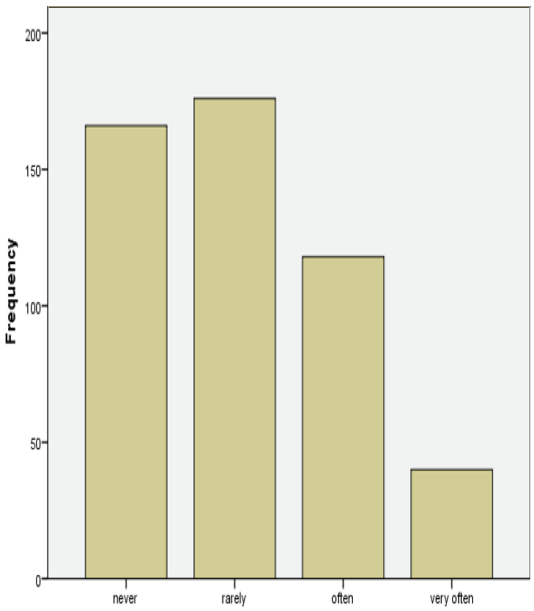

Fig. 2. Frequency of password sharing.

TABLE III
DANGEROUS PRACTICES BY USERS

Institution	Public Wi-Fi (%)		License agreement (%)			Password sharing (%)		Information storage (%)	
	Yes	No	Yes	Sometimes	No	Yes	No	Yes	No
University of Jos	100	0	8	31	61	66	34	58	42
Plateau State Polytechnic	48	52	56	28	16	75	25	61	39
NTA College	46	54	51	23	26	41	59	67	33
College of Forestry	97	3	0	18	82	64	36	62	38
College of Health	49	51	57	20	23	26	74	63	37
Total	68	32	34.4	24	41.6	44.4	55.6	62.2	37.8

Figure 3 shows the distribution of respondents who consider themselves responsible for the security of their devices and those who do not.

Majority of the users believe that they have the responsibility to provide maximum defense for their mobile devices and the sensitive information stored in them. This is supported by the result of the survey as 79.2% (396) respondents consider themselves responsible for the security of their devices. This makes the job of security professionals easier as many respondents are ready to take measures to protect their devices. The rapid increase in mobile applications and the ease with which they can be downloaded via platforms such as Google play, Play Store and AppStore enable respondents to make regular use of such applications. A large number of respondents do not read the End-User License Agreement (EULA) before installing applications. It is interesting to note that 311 (or 62.2%) respondents who store sensitive information on their devices do not read end user license agreement when installing

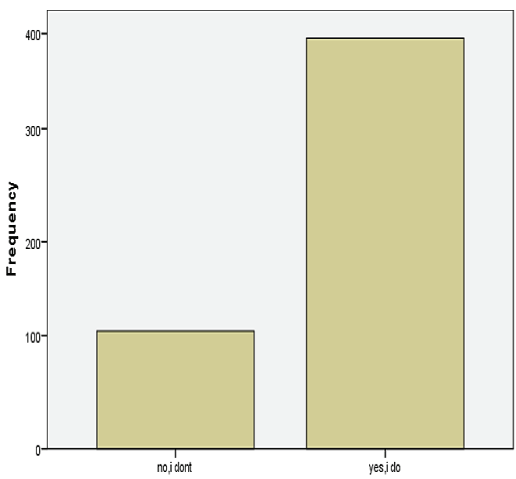

Fig. 3. Responsible for device security.

mobile applications. Table 3 shows that 41.6% (208) of the respondents do not read the EULA before installing applications on their mobile devices. This is a bad practice as mobile devices are highly vulnerable to threats. This means that a significant number of users are unaware of the implications of giving permissions to applications on mobile devices. On the other hand, 172 (34.4%) participants pay attention to what the installed application can access, execute and activate on their devices, while 120 (24.0%) sometimes read the license agreement when installing an application.

D. Security Knowledge and Concern

This section presents results related to human behaviors, knowledge and concerns from the perspective of mobile security awareness. A few questions were asked to measure level of concern about device security and user's awareness of information security. Table 4 presents the survey results for the various institutions.

TABLE IV
SECURITY KNOWLEDG AND CONCERN

Institution	Device knowledge (%)		Security importance (%)			Security concern (%)			Website identification (%)		Credit card usage (%)		Security verification (%)	
	Yes	No	Yes	No	Somehow important	High concern	Little concern	No concern	Yes	No	Yes	No	Yes	No
University of Jos	62	38	79	1	20	84	31	3	24	72	17	83	4	94
Plateau state polytechnic	51	49	87	1	12	50	31	19	46	54	44	56	23	77
NTA Television College	48	52	93	0	7	62	26	12	38	62	39	61	22	78
College of forestry	22	78	78	0	22	73	27	0	25	75	17	82	0	100
College of health	49	51	91	1	8	48	36	16	42	58	33	67	23	77
Total	58.4	41.6	85.6	0.6	13.8	63.4	27	9.6	35	65	30.1	69.9	85.6	14.4

Majority (58.4% or 285) of the respondents know about the security of their mobile devices, while 41.6% (215) do not. This is a positive result in terms of physical security and technical security. A sizeable number of respondents are strongly concerned about the security of their devices when making transactions on the Internet. The table shows that about 317 (63.4%) have keen interest, 135 (27%) are a little concerned and 9.6% are not concerned at all. This is a positive indicator as majority acknowledged device security as a paramount issue. It was also observed that some students have either lost or misplaced their bank cards at one time or the other. Hence, they are careful when using mobile applications. A large number of respondents (349 or 69.9%) are not favorably disposed to using their credit cards on the web. These students would not conduct any online transaction such as banking without a statement from the bank on the security procedures to be used. It was a surprising to discover that majority of the respondents cannot distinguish a secured website from an insecure one. Table 4 shows that about 325 (65%) respondents do not know the difference between a secure and insecure website, while a handful (175 or 35%) of them know. This is further proven by the responses gotten when a question was asked about whether they use public Wi-Fi or not as in Table 3. A total of 340 (or 68%) respondents use public Wi-Fi, while 32.0% (160) do not. Majority of the users (85.6% or 428 respondents) believe that mobile device security is important, while 13.8% think the security of their device is somewhat important. About 0.6% do not believe that it is important to secure their devices.

V. CONCLUSION AND FUTURE WORK

The widespread use of smart phones and other mobile devices has greatly increased the security concerns of the users of these devices. The concern is heightened by the fact that many people store sensitive personal information on mobile devices, while a sizeable number of mobile devices owners use their gadgets. The sensitive nature of information stored on or transmitted via mobile devices and the limited knowledge of security among mobile device owners makes it imperative to take necessary steps that increase security awareness and knowledge of mobile device users. This study explored the differences in perception and levels of security awareness level among students who own mobile devices in selected tertiary institutions in Plateau State. Findings from the study showed that many students (58.4%) have good knowledge of the features and functionalities of their devices. Many of them (85.6%) also believe mobile device security important and a large proportion (63.4%) have genuine security concerns. The study revealed that academic literacy does not automatically translate to security knowledge. For example, a sizeable proportion (35%) does not know the differences between legitimate and malicious websites, while many of them (30.1%) store sensitive information such as financial records and credit card details on their mobile devices. Many of these highly literate users are not aware of the implications of their actions and inactions on the security of their devices and information stored in them. Students should be enlightened on the need to secure their mobile devices. They should be informed about security measures and encouraged to store sensitive information in the cloud instead of mobile phones. The enlightenment may be in the form of text messages (sent to their

phones regularly), periodic seminars or specialized trainings that broaden their knowledge on mobile device security and prevent them from becoming victims of identity theft, fraud or other forms of sabotage. In the future, researchers will look into the level of mobile device security awareness among the non-students and local communities, in plateau state and the north central region of Nigeria.

REFERENCES

[1] "How Many Smartphone Are in the World?" https://www.bankingmycell.com/blog/how-many-phones-are-in-the-world

[2] L. Handley, "Nearly three quarters of the world will use just their smartphones to access Internet by 2025," https://google.com/amp/s/www.cnbc.com/amp/2019/01/24/smartphones-72percent-of-people-will-use-only-mobile-for-Internet-by-2025.html, Month 2019.

[3] Statisca, "Nigeria: mobile internet users 2016-2026," https://google.com/search?q=number+of+mobile+Internet+users+in+Nigeria+2021&oq=number+of+mobile+Internet+users+in+niger&aqs=chrome.3.6.9i57j33i22i29i3014.26132joj4&sourceid=chrome-mobile&ieUTF-8, Month 2021.

[4] A. Adepetun, "Cyber threats to mobile devices in Nigeria rise, hit 35%," https://guadian.ng/technology/cyber-threats-to-mobile-device-in-nigeria-hits-35/, Month 2018.

[5] J.M. Stanton, P.R Mastrangelo, K.R Stam and J. Jolton, "Analysis of the end user security behaviors," Computers and Security, vol. 24, no. 2, pp. 124-133, Month 2005.

[6] A. Khalfan, "Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors," International Journal of Information Management, vol. 24, no. 1, pp. 29-42, Month 2004.

[7] L. Handley J. Khan, H. Abbas and J. Al-Muhtadi, "Survey on mobile user's data privacy threat and defense mechanisms," International Workshop on Cyber Security and Digital Investigation (CSDI 2015), Procedia Computer Science, vol. 56, pp. 376-383, Month 2015.

[8] M. Zeybek, E.N. Yilmaz and I.A. Doğru, "A study on security awareness in mobile devices," 1st International Informatics and Software Engineering Conference (UBMYK) pp.1-6, Month 2019.

[9] H. Susanto "Revealing cyber threat of smart mobile device within digital ecosystem: user information security awareness, data integrity and quality, IntechOpen, pp. 1-26, 2021.

[10] O. Kulyk, B. Reinheimer, L. Aldag, P. Mayer, N. Gerber and M. Volkamer, "Security and privacy awareness in smart environments- a cross-country investigation," Financial Cryptography and Data Security, Springer International, pp. 84-101, Month 2020.

[11] A. G. Chin, U. Etudo and M.A. Harris, "On mobile device security practices and training efficacy: an empirical study. informatics in education," vol. 15, no.2, pp. 235-252, Month 2016.

[12] M.N.Y. Ali, M.L. Rahman and I. Jahan, "Security and privacy awareness: a survey on smartphone user," International Journal of Advanced Computer Science and Applications, vol 10, no. 9, pp. 222-226, September 2020.

[13] A. Rufai, S. Modi and B. Wadata, "A survey of cyber- security practices in Nigeria," International Research Journal of Advance Engineering Science and Application, vol. 10, no 9, pp.483-488, September 2019.

[14] M. Koyuncu and T. Pusatli "Security awareness level of smartphone users: an exploratory case study," Mobile Information Systems, vol 2019, pp. 1-11, Month 2019.

[15] E.E. Eguzoikpe, Research Methodology: A Practical Treatise for Students. Jos, Nigeria: Quality Functions Publishers, 2008.

Abayomi Jegede is an Associate Professor in the Department of Computer Science, University of Jos, Nigeria. He is also an instructional facilitator and research advisor at African Centre of Excellence on Technology Enhanced Learning (A World Bank Assisted Centre of Academic Excellence) domiciled in National Open University of Nigeria. He received his BSc and MSc degrees in Computer Science from University of Ibadan Nigeria. He also obtained a PhD in Security in Computing from Universiti Putra Malaysia. Dr. Jegede is an EC-Council Certified Ethical Hacker and Computer Hacking Forensic Investigator. He is a member of several professional bodies including Association for Computing Machinery (ACM), ACM special interest group on security, audit and control ACM SIGSAC), Internet Society of Nigeria, Computer Professionals (Registration Council) of Nigeria and the Society for digital and wireless communication. He is also a Fellow of Nigeria School of Internet Governance. He has authored several papers in the areas of biometric security, IoT Security, network security and broad areas of computer science. His research interests include design and implementation of secure biometric systems, AI applications in cyber security and computer forensics and cyber terrorism and information warfare.

Grace Odii holds a BSc degree in Computer Science from University of Jos. Her research interests include information security and computer forensics.

Musa Magaji is a program manager at Bindir Knowledge Center Yola. He is also a postgraduate student of the Department of Computer Science, University of Jos, Nigeria. He received his BTech degree in Computer Science from Modibbo Adama University of technology Yola, Nigeria. His research interests include ML applications in cyber security and Network administration.

Gilbert Aimufua ia an Associate Professor of Computer Science Nasarawa State University, Keffi, Nigeria. He received his BSc and MSc degrees in Computer Science from University of Lagos, Nigeria. He also holds a PhD degree in Information Technology jointly awarded by Accra Institute of Technology, Ghana/Open University Malaysia. His research interests include applied information systems and software engineering. Dr. Aimufua has published several papers in computer science and information systems.