International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No.41, October 2023 – www.ijais.org

Privacy and Security Issues: An Assessment of the Awareness Level of Smartphone Users in Nigeria

Omeka Friday Odey
Department of Computer Science, Faculty of Computing, Federal University of Lafia P.M.B 146 Lafia, Nigeria

Joshua Abah
Department of Computer Science, Faculty of Computing, Federal University of Lafia P.M.B 146 Lafia, Nigeria

Dekera Kenneth Kwaghtyo
Department of Computer Science, Faculty of Computing, Federal University of Lafia P.M.B 146 Lafia, Nigeria

ABSTRACT

The use of smartphones in Nigeria has continued to increase daily and worsened during and after the Covid-19 pandemic that locked down even the developed nations. Like computers, smartphones keep the memory of users' details like account details and transaction histories including passwords of their social media platforms. The huge volume of data being stored by smartphones brings about an unlimited number of privacy and security challenges. That is, security threats perpetrated by malicious actors or hackers is proportional to the ubiquity and adoption of smartphone in Nigeria. Therefore, this study aims to assess the awareness level of smartphone users in Nigeria regarding privacy and security issues associated with smartphones. By so doing, the study surveyed smartphone users across the 36 states and the FCT in Nigeria. The study employed both quantitative and qualitative methods. The quantitative research approach was utilized for data collection. While the qualitative approach was leveraged for descriptive analytics. The analysis was performed using the Statistical Package for Social Science (SPSS) to provide the graphical results. An existing mathematical model was therefore adapted and utilized to calculate the awareness level of smartphone users. The analytical outcome of the survey revealed that a considerable number of smartphone users in Nigeria are unaware of privacy and security issues allied to smartphones.

General Terms

Data and Information Security, Mobile Device Security, Cybersecurity Awareness.

Keywords

Smartphone, Smartphone-threats, Awareness Level (AL), Privacy/Security.

1. INTRODUCTION

Privacy and security threats on mobile devices are unauthorized attempts to invade, retrieve, disrupt, degrade or destroy sensitive data stored or transmitted via devices [1], [2]. The ubiquity and adoption of mobile devices have revolutionized worldwide access to information, communications, and how tasks can be done. In recent time, this has worsened the security threats and attacks on smartphone users. In Nigeria, according to the Nigerian Communications Commission (NCC), the total number of mobile subscribers rose to 221,258,372 million in May 2023, from 149,249,510 million in April 2017 [3]. This reflects the deep penetration and widespread adoption of mobile devices in Nigeria, with the increasing number of young people and the growing demand for digital services. Globally, about 6.4 billion mobile devices are in use and this figure is projected to rise to 7.7 billion by 2028, Countries like China, India, and the United States are rated as having the highest number of Smartphone usage in the world [4]. This extensive adoption of mobile devices is driven by their availability, lightweight, and versatility [5]. Internet connectivity has also improved, making it possible for people in remote areas to have access to digital services. Additionally, the versatility of mobile devices, with the availability of various apps and services, has made them essential for communication, productivity, entertainment, and learning [6].

The worldwide acceptability of mobile devices has attracted several security and privacy issues attributed to the amount of personal data stored on these devices [7]. Some of the security and privacy issues with mobile devices include Data breaches, Malware and ransomware attacks, Phishing and social engineering attacks, App vulnerabilities, and Physical theft and loss [8]. These issues are challenging and life-threatening to individuals, businesses and the government. For instance, the invasion of third-party applications that collects and misuse personal data [9]. Some of this software exploit and create vulnerabilities that are beneficial to hackers or any malicious actor.

One driving factor contributing to the increasing number of privacy and security issues is the lack of user awareness of associated threat vectors in mobile devices [10]. Researchers emphasized that poor knowledge of mobile device security threats by users has posed significant damage [11]. Lack of awareness and the inability of users to protect their Smartphones and data have continued to gain exceeding rise to different forms of attacks [12]. Also, the unnoticed vulnerabilities created at the design stage which users of these devices are completely unaware of the danger before them [13] hence become a feast for attackers to prey. As a result, the Bring Your Own Device (BYOD) policy of carrying out corporate-related tasks [14], [15] using personal devices poses more risk due to unawareness of the vulnerabilities associated with devices.

Quite several existing studies have been conducted to assess the awareness of privacy and security threats of mobile device users in Nigeria [10], [16]–[18]. However, these studies delve into mobile security awareness on a very broad aspect. Particularly, the studies investigated cyber security awareness levels irrespective of the kind of device owned. Additionally, they employ descriptive analysis to demonstrate privacy and security awareness level. Likewise, the most recent study [18]. On machine learning, the authors [19] developed a behavioural-based scheme for the security of smartphones against unknown attacks also termed zero-day attacks. Conversely, this study employed both qualitative and quantitative research approaches to investigate the level of privacy and security awareness particularly for Smartphone users. Majorly, the study demystified the belief that Smartphone users are savvy about the associated privacy and security threats. Also checked is the correlation between the literacy level of Smartphone users to privacy and security awareness level. A large number of participants cutting across diverse backgrounds, faith and exposure in Nigeria is covered in this study. Since various studies have proven that privacy and security threat is increasing exponentially in their regions [10], [16]–[18]. Thus, this study provides a state-of-the-art baseline that other researchers can leverage. The study seeks to address the following research questions:

- Do you use a screen lock (e.g. pin, pattern or fingerprint?
- Do you save passwords in any location of your device or email?
- Have you enabled 2FA authentication on your mobile device to provide an extra layer of security?
- Do you update and use different passwords for different accounts?
- How concerned are you about the privacy and security of the information on your mobile device?
- Do you review the privacy policy before granting App permission?
- Do you know what type of information that is collected from your device by third-party Apps?
- Are you aware of the danger of self-disclosure of personal data?
- Are you aware of the potential risk of using public Wi-Fi Networks on your device?
- Have you entered a site despite a security warning that the site is dangerous?

The remainder of this study is prearranged thus. Section 2 dwells on related works. In section 3 the research method employed is described. Section 4 presents and discusses the results. In section 5 the findings of the study are outlined. Lastly, section 6 provides the conclusions drawn from the study.

2. REVIEW OF RELATED WORKS

Privacy and security awareness levels of Smartphone users have gained researchers' interest hence widely considered across the regions of the globe. For instance, the authors [20] conducted a study investigating the security consciousness of Smartphone users through an exploratory analysis. A sample of 155 Smartphone users was gathered in Turkey for the analysis. The study found that the security awareness level of Smartphone users was low in terms of age, the older group has a lower awareness level compared to the younger group. Similarly, [21] conducted a study assessing Smartphone users' security choices, awareness, behaviour, and education. The findings obtained from 204 participant shows that most users are aware of some security practice such as using suitable screen lock settings to safeguard against unauthorized access. The measure of the knowledge and level of security awareness of Smartphone users in Indonesia on information security and privacy was also conducted [22]. The results show a low awareness level in terms of threats and attacks. This indicates that there are still a lot of mobile users in Indonesians who are not aware of the security and privacy of their smartphones. Especially, in regards to taking cognizance of the significance of reading privacy policies.

In South Africa, the researchers [23] carried out a study to evaluate factors that influence mobile users' security behaviours. The authors leveraged the KAB and TPB models using a sample size of 397 participants who are students from selected higher institutions. The results show a noteworthy correlation between understanding and the intention to act against security threats. Also, the existence of a gap between knowledge of security and commitment to safety behaviours is demonstrated**.** This explains the concept of “knowing versus doing”, Where students' knowledge of information security does not translate into adopting secured security behaviours. The study suggested more awareness creation through training and educating the students to combat security issues. An empirical study was conducted by [24] to evaluate the cyber security behaviour and practices of smartphone users in India with 300 participants. The study revealed that respondents did not exhibit good cybersecurity behaviours, though users have adopted some of the most popular security features such as screen lock on their smartphones. However, they are not aware of certain technical security controls such as encryption and remote wipe. It was also discovered that there are significant gaps between behaviour and practices. Thus, the participants reported a high level of motivation to protect their devices and data. Whereas, they reported a moderate level of threat awareness and the ability to protect their device and data. In a related manner, a total of total 504 participants were utilized to carry out a study on Smartphone security behaviours and practices of users [25]. The result shows that users exhibit a high degree of care on some measures of security. However, they are rather lax in other areas such as downloading applications from un-trusted sources, using weak passwords, and sharing sensitive information.

In Nigeria, the researchers [10] conducted a study examining the extent of cyber security awareness of mobile device users across five tertiary institutions in Plateau state, Nigeria. A sample size of 397 respondents was collected and analyzed using descriptive statistics. The results reveal, that a large number of students have good and genuine security concerns and believe in the importance of mobile device security. On the other hand, the study also revealed that being educated does not habitually mean you're aware and conscious of security issues. For instance, a significant number of students do not know the variances between genuine and harmful websites, and many of them store sensitive data such as transaction history and credit card details on their smartphones. Similarly, the authors [16] investigated the level of awareness of cybercrime among mobile device users in Imo State. Over 1031 respondents took part in the survey. Analytical results show that the number of cybercrimes is more computer-related crimes like e-theft than computer-focused crimes like spam mail. Again, the view and level of awareness of mobile device users concerning cyber security issues in Nigeria were surveyed in the study [17]. The study which utilized a total of 40 respondents to perform the analysis revealed that a considerable number of Nigerians are aware of the fundamental cyber security concerns. Also, in the North Eastern part of Nigeria, the researchers [18] utilized over 441 respondents out of the returned 500 participants. Demographically, over 77.1 % are male students and 22.9 % are females. The study exposed that there is a moderate awareness level of cybersecurity among the students in the region.

3. MATERIALS AND METHODOLOGY

To evaluate the level of privacy and security awareness of Smartphone users in Nigeria. Both quantitative and qualitative research approaches were employed. While the earlier was used for analytical purposes, the latter was utilized to describe the analytical results. The methods and materials employed in the study are briefly described in the following subsections.

3.1 The Survey Approach

Various steps have been considered to arrive at the findings of the survey. These steps are described as follows:

1) Firstly, a comprehensive review of related work was carried out which provided the bearing and significance of the survey.
2) Secondly, a Google form was created to collect key information such as privacy and security issues, the kind of tasks, passwords and authentication mechanisms Smartphone users employ to safeguard their devices.
3) Thirdly, the link to the Google form arrived at was shared across various social media platforms like WhatsApp, Facebook, Messenger, and Twitter including student and staff forums across the country.
4) The data acquired was carefully analyzed using the Statistical Package for Social Sciences (SPSS).

3.2 The Survey Design Tool

Data being a key aspect of survey research was given its worthwhile time. The instrument used for collecting data for the validation of this study is the Google Form which is one of the most commonly used methods for data collection. Though, it has some relative limitations which according to [26] takes time and is also expensive, especially when the survey coverage area is very large as in this case. The questionnaire contains 50 logical and distinct questions, with headings specifying each category of questions. All the questions were based on the privacy and security awareness of Smartphone users. Among the 50 questions, 10 questions that can address and fulfil our objectives were carefully selected for analysis and discussion. The questionnaire was passed through various editions to arrive at concise/precise survey questions to provide answers to the research questions raised. The authors carefully followed the standards for formulating questionnaires to enhance truthful responses. Table 1 shows the sample of the research hypotheses derived from the research questions possible to gain knowledge of the awareness level of Smartphone users.

Table 1. The study hypothesis

s/n	Hypothesis
H01	There is no significant difference in security and privacy practices between users who activate screen lock (e.g., pin, pattern, or fingerprint) on their Smartphones and those who do not employ any.
H02	There is no significant difference between Smartphone users who save passwords in any location of the device or email and those who do not.
H03	There is no significant difference between Smartphone users who enabled 2FA authentication on their devices to provide an extra layer of security and those who do not.
H04	There is no significant difference in the ratio of Smartphone users who update and use different passwords for different accounts compared to those who do not.
H05	There is no significant difference in the level of concern about the privacy and security of information among Smartphone users.
H06	There is no significant difference between Smartphone users who review privacy policies before granting App permissions and those who do not.
H07	There is no significant difference between Smartphone users who know what type of information is collected from their device by third-party Apps and those who do not.
H08	There is no significant difference in the level of awareness of the danger of self-disclosure of personal data among Smartphone users.
H09	There is no significant difference in the level of awareness of the potential risk of using public Wi-Fi networks on mobile devices among Smartphone users.
H010	There is no significant difference between Smartphone users who have entered a site despite receiving a security warning that the site is dangerous and those who have not.

3.3 The Target Population

The targeted population for the study is Smartphone users across the 36 states and the Federal Capital Territory (FCT) of Nigeria ranging from 13 to 65 years of age and above. Participants were invited across Nigerian states and the FCT using the crowd-sourcing method [26] of sharing the survey link via social media handles like Facebook, WhatsApp and Telegram including email and a non-social media platform (SMS). The survey duration lasted for one year and one month which spanned from May 2022 to June 2023.

3.4 Determining of Awareness Level (AL)

This study adopted the procedure utilized by [26], [27] to determine the awareness level of Smartphone users in Nigeria. The utilized Awareness Level formula is given by:

$$AL = 1 - \left(\frac{2}{1 + \mathrm{e}^{-\mathrm{H}}} - 1\right) \qquad (1)$$

Where: AL = Awareness Level, H = sum of all values for each hypothesis. The symbol e is an exponential constant which is approximately 2.718. When converted to a percentage, this equation gives 100 % of all the participants choose the safe answers for all the questions. Whereas, it gives 0 % if Smartphone users select all the unsafe answers.

4. DISCUSSION OF RESULTS

This section presents and analyzes the outcome of the survey using the data gathered in the course of the study. Before going into analysis, a total of 11,035 respondents took part in filling the survey questionnaire (google form) online, within 11 months. Out of these 215 responses were filtered out because some questions were made to be free responses. As such, respondents did not supply reasonable answers to them maybe due to illiteracy or insincerity. Thus, those rows of entries were considered to be invalid entries and hence removed the data. Consequently, 10820 responses were utilized for analysis.

4.1 Demographic Analysis

Based on the demographic data provided in the survey, 74.7 % of the respondents who use Smartphones are young people between the age of 18-35. While the remaining 25.3 % cut across four different age groups which are 13-17; 36-45; 46-65; 66 and above. Gender-wise, 59.0 % of Smartphone users are male and the remaining 40.3 % are female. The remaining 0.8 % preferred not to disclose their gender. In terms of educational attainment of Smartphone users, 86.1 % of the respondents attained tertiary education. The secondary and primary level of education has 13.3 % and 0.7 % respectively. Also, 62.1 % of the respondents are students while 18.0 % of Smartphone users are unemployed. The remaining 19.9 % of the participants are either Federal, State, NGO, or Private (self) employed. Table 2 shows the demographic details of the respondents.

Table 2. Participants' demographic details

Age	Percentage (%)
13-17	4.4
18-35	74.7
36-45	12.3
46-65	3.7
65 and Above	4.8
Gender	**Percentage (%)**
Female	40.3
Male	59.0
Prefer not to specify	0.8
Educational Level	**Percentage (%)**
Primary	o.7
Secondary	13.3
Tertiary	86.1
Employment Status	**Percentage (%)**
Federal Staff	2.6
NGO Staff	3.0
Not Employed	18.0
Private Staff	7.4
State Staff	6.8
Student	62.1

4.2 Analysis Based on the Research Hypothesis

4.2.1 H01: There is no significant difference in security and privacy practices between users who activate screen lock (e.g., pin, pattern, or fingerprint) on their Smartphone and those who do not employ any

Figure 1 represents the above hypothesis (H01). It is concerned with users who adopt the use of screen lock security mechanisms on their Smartphones to limit unauthorized access and those who do not. It can be observed that 83.45 % of the respondents have been using screen lock, while 16.55 % do not use screen lock. Having 83.45 % of Smartphone users adopt the use of screen lock is an indication that a significant number of Smartphone users are aware of the importance of securing their devices and data from theft. However, the 16.55 % of Smartphone users that do not use screen lock can be attributed to a lack of awareness of the associated consequence. This survey analysis demonstrated that there is a significant difference between Smartphone users in terms of privacy and security of their devices.

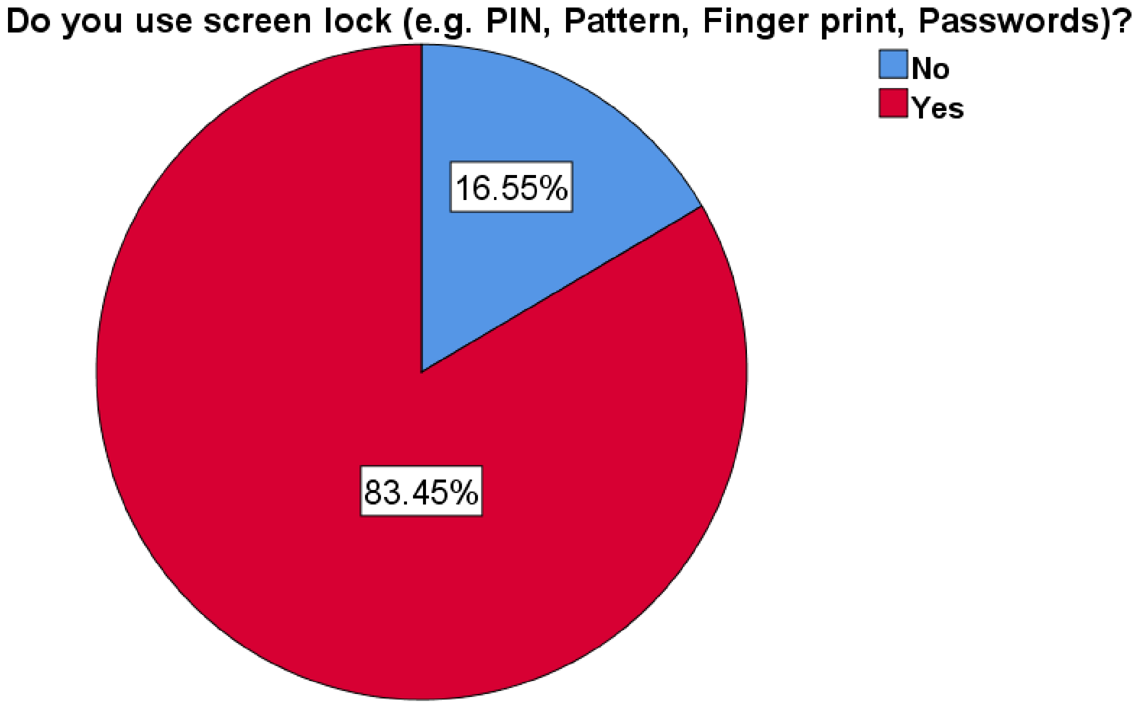

Figure 1: Participants' usage of screen lock

4.2.2 H02: There is no significant difference between Smartphone users who save passwords in any location of the device or email and those who do not.

Hypothesis two (H02) assesses whether Smartphone users keep track of activities like passwords and financial details. Figure 2 illustrates that 57.20 % of the respondents do not save their secret codes on any location or email. While 39.24 % do save their login credentials on any location including email. About 3.56 % of Smartphone users could not remember whether or not they must have saved. This shows that over 42.8 % who keep records of their passwords or who are not sure of keeping such records are more prone to security threats. There is a relative difference between smartphone users who save passwords in different locations on their smartphones and those who do not.

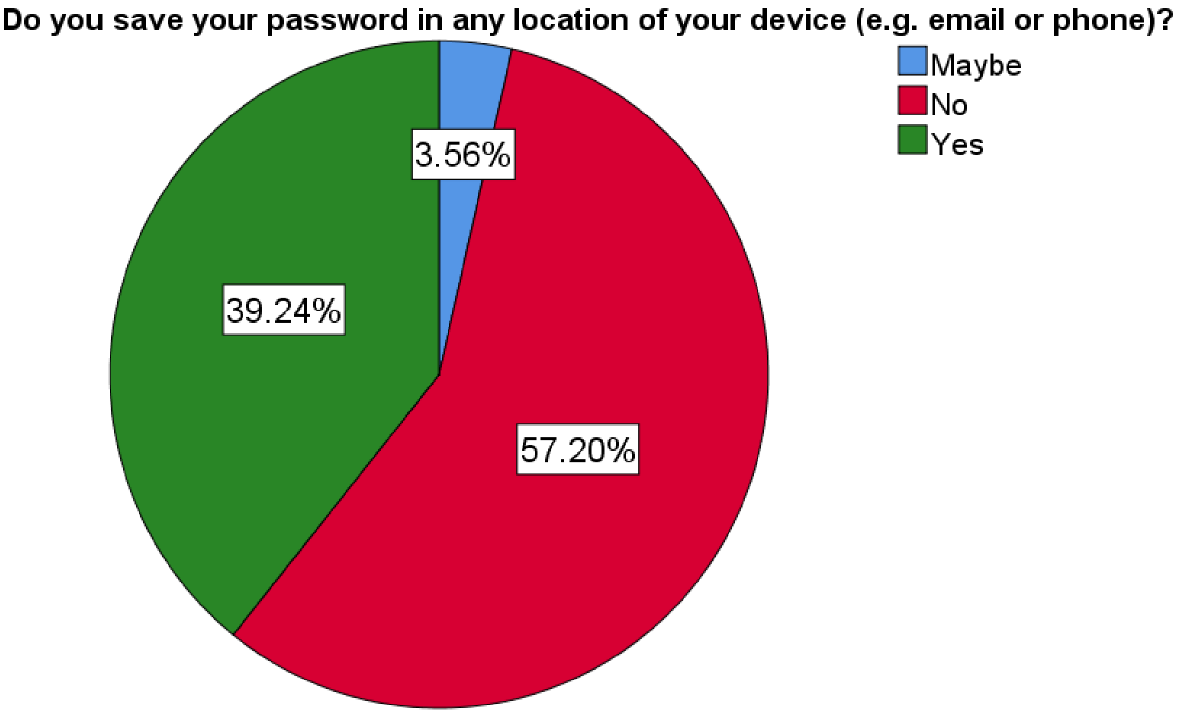

Figure 2: Participants' storage of passwords on their smartphone or email

4.2.3 H03: There is no significant difference between Smartphone users who enabled 2FA authentication on their devices to provide an extra layer of security and those who do not

Two Factor Authentication (2FA) is a second-level or additional authentication mechanism for securing devices and users' accounts from unauthorized access. As such, hypothesis three (H03) assesses the number of Smartphone users who have enabled 2FA authentication on their smartphones to provide an extra layer of security and those who do not. Based on the data illustrated in Figure 3, about 68.25 % of the respondents do not enable 2FA authentication. While 30.96 % of smartphone users do enable 2FA and 0.79% are not sure whether or not there have implemented 2FA on their Smartphones. It can be deduced here that 68.25 % of Smartphone users are less secure compared to 30.96 % and 0.79 % of respondents.

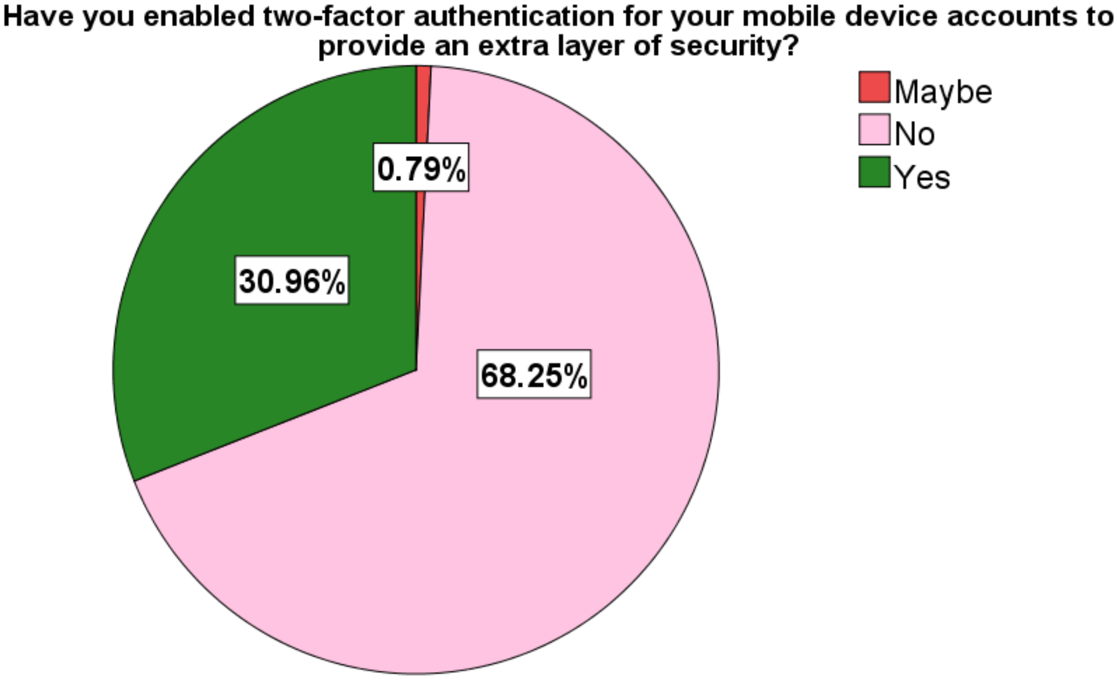

Figure 3: Participants' knowledge of 2FA authentication on their Smartphones

4.2.4 H04: There is no significant difference in the ratio of Smartphone users who update and use different passwords for different accounts compared to those who do not

Updating or changing passwords or any login credentials is a good approach toward securing one's device against third-party or unauthorized access. Hypothesis four (Ho4) weighs the number of Smartphone users who constantly update their passwords or use different passwords for different accounts. As captured in Figure 4, more than 53.96 % of the respondents are victims of using the same password across applications without updating or changing it. While only 46.04 % of smartphone users do update and use different passwords on different accounts/applications. This is an indication that 53.96 % of Smartphone users are less secure and unaware of the risks attached to their actions than 46.04 % of users.

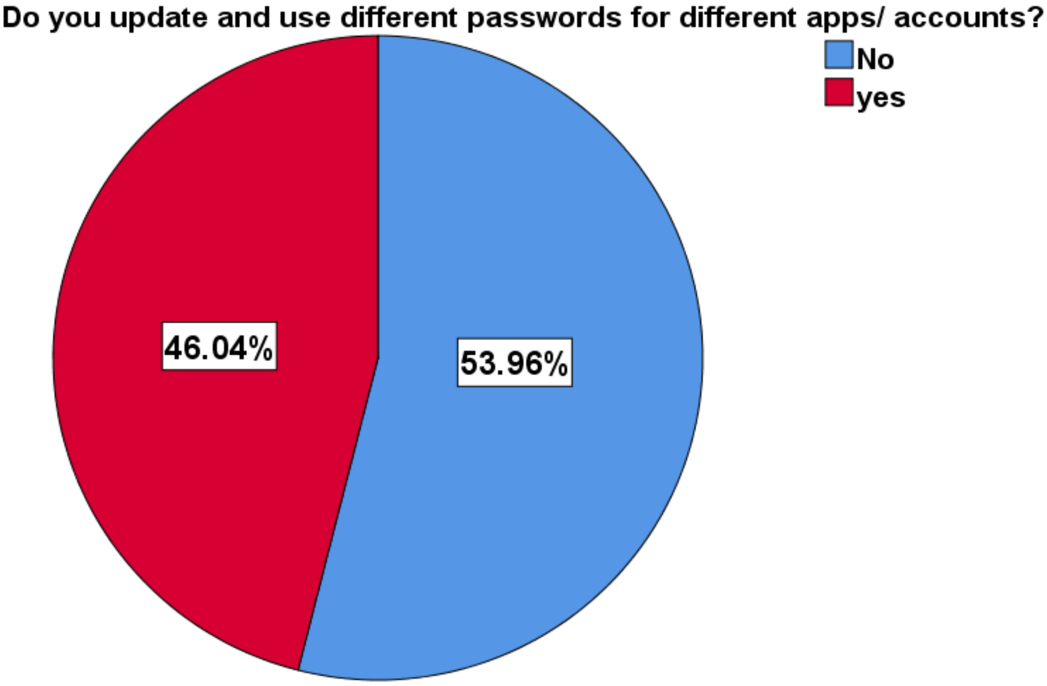

Figure 4: How participants update or use different passwords

4.2.5 H05: There is no significant difference in the level of concern about the privacy and security of information among Smartphone users

Hypothesis five (H05) considers the number of Smartphone users who are concerned about or not Smartphones. Figure 5 shows the analysis of those who are concerned or not concerned about the privacy of their devices. 60.66 % of the respondents are concerned while 39.34 % of Smartphone users admitted not having any concern about the security of their devices. This demonstrates that over 39.34 % of Smartphone users are prone to security threats and attacks due to unawareness.

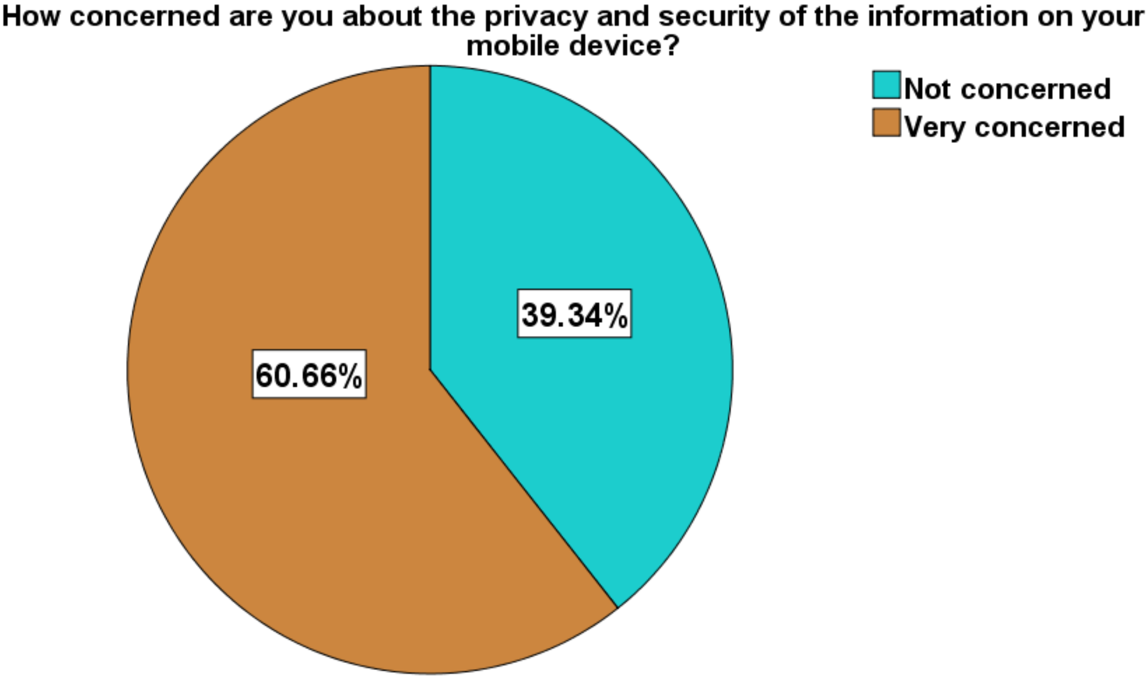

Figure 5: Participants who are concerned about privacy and security

4.2.6 H06: There is no significant difference between Smartphone users who review privacy policies before granting App permissions and those who do not

Hypothesis six (H06) is concerned with permission requests by applications when Smartphone users attempt to install new applications. Permission requests seek to access sensitive data available on the user's device. Data can only be accessed by third-party applications if such permission requests are granted.

The analysis in Figure 6 is a reflection of Smartphone users who review and who do not review app permissions before granting access. From the analysis, 78.80 % reject, 20.35 % accept and 0.85% are not sure of accepting or rejecting permission requests from third-party applications. This implies that over 21.20 % of Smartphone users are far less secure and completely not aware of the risks associated with application permission requests.

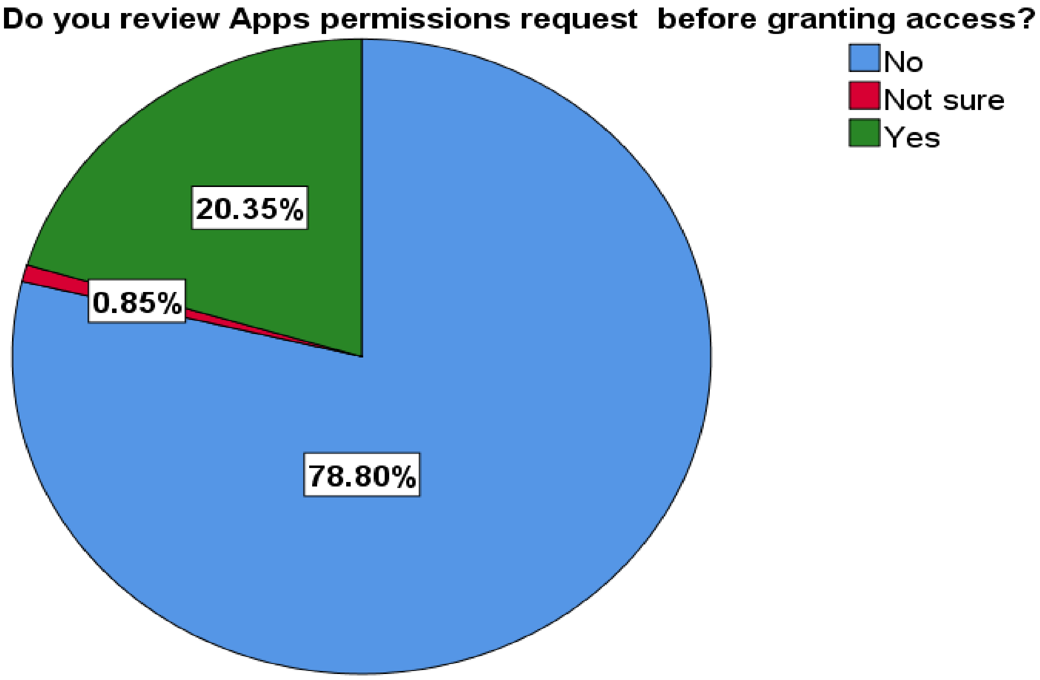

Figure 6: Participants' approaches towards Apps permission requests

4.2.7 H07: There is no significant difference between Smartphone users who know what type of information is collected from their device by third-party Apps and those who do not

Hypothesis seven (H07) assesses the awareness level of Smartphone users concerning the type of information third-party applications collect from their devices. The survey analysis provided that a significant number of users' lack awareness. That is, 90.26 % of the respondents agree to lack awareness of the possible data that can be collected from their device. Meanwhile, only 9.74% of the respondent agree to be aware. The 90.26 % is quite high and calls for serious action. The implication is that when users lack awareness of key issues, their ability to manage and control their data become difficult.

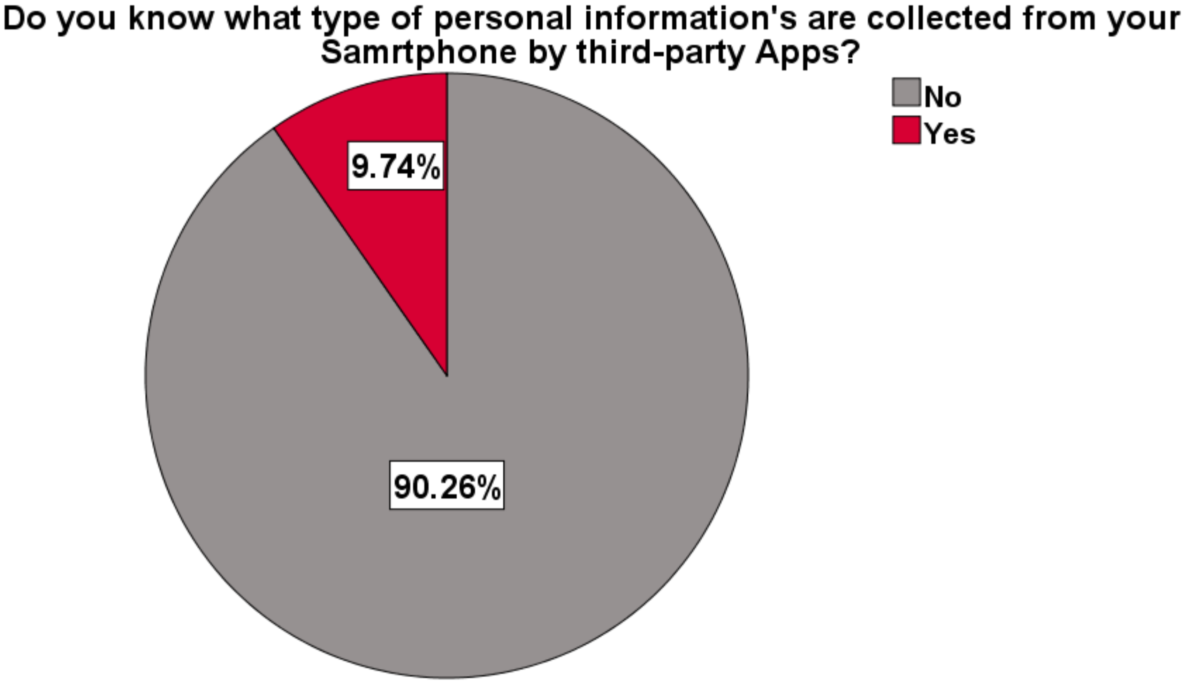

Figure 7: Participants' knowledge of information collected by third-party Apps

4.2.8 H08: There is no significant difference in the level of awareness of the danger of self-disclosure of personal data among Smartphone users

Disclosure of personal details is risky, based on the survey findings, 80.96 % of the respondent are not aware of the danger of self-disclosure of personal information. This significant number of respondents lack an understanding of the potential risk associated with sharing personal details across social media platforms. This can result in potential consequences such as privacy breaches, cyberbullying, identity theft and other forms of attacks. On the other hand, 14.01% of the respondents admitted being aware of the implications and the risks of self-disclosure of information. This can build consciousness and limit them from being exposed to security attacks. Again, 5.03 % of the respondent are likely to fall, victim, because they probably lack the right knowledge or risk of self-disclosure.

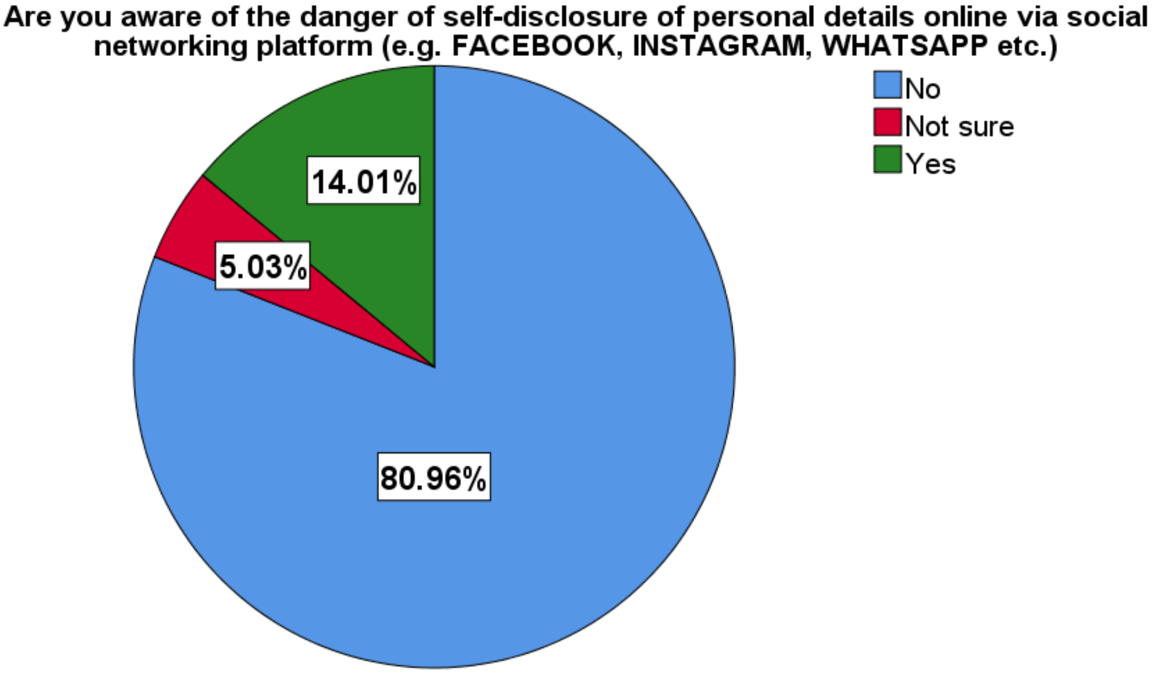

Figure 8: Participants' knowledge of the risk of self-disclosure of information

4.2.9 H09: There is no significant difference in the level of awareness of the potential risk of using public Wi-Fi networks on mobile devices among Smartphone users

Using public Wi-Fi can be very enticing because users can access the internet at no personal cost. Again, most public Wi-Fi is generally less secure. Thus, using them, login credentials can be at risk of interception and exposure to middlemen attacks where malicious actors can perform eavesdropping attacks. An attacker can also set up a fake Wi-Fi network similar to a legitimate network, tricking users to connect to their malicious network. The above hypothesis nine (H09) seeks the awareness of Smartphone users about public Wi-Fi risks. Figure 9, therefore, provides the analytical information using the survey data. 62.79 % of the respondent are not aware of the associated risks of using public Wi-Fi. While only 37.21 % of the respondents are aware of the risks attached to the use of public networks (Wi-Fi). This analysis has demonstrated a great significant difference between users of public Wi-Fi and those who do not.

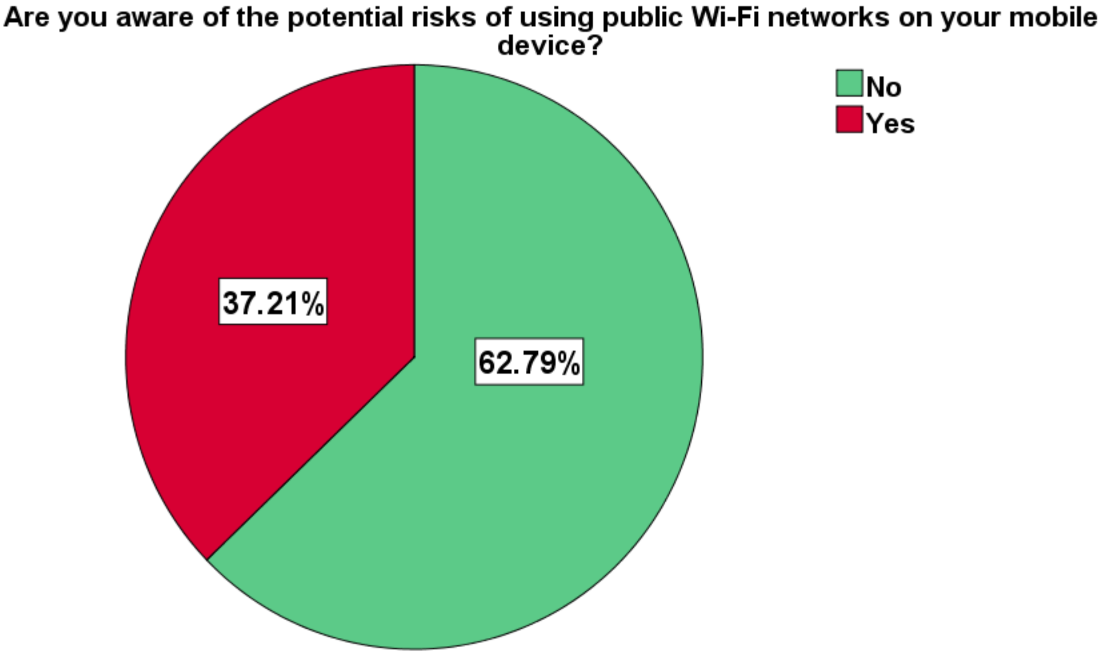

Figure 9: Participants' knowledge of Wi-Fi network risks

4.2.10 H010: There is no significant difference between Smartphone users who have entered a site despite receiving a security warning that the site is dangerous and those who have not

Hypothesis ten (H010) assesses users' attitudes towards entering sites despite security warnings that the site is not secure. The analysis provided in Figure 10 shows that 65.53 % of the respondents ignore the security warning and proceed to websites, and 20.48 % adhere to the security threat alerts. While 13.99 % are uncertain about accessing websites when having received or seen an indication of a safety signal. With 65.53 % admitting to having proceeded despite security warnings is a clear indication that a lot of users are less secure. This behaviour can be attributed to a lack of awareness of the severity of the risk associated therewith.

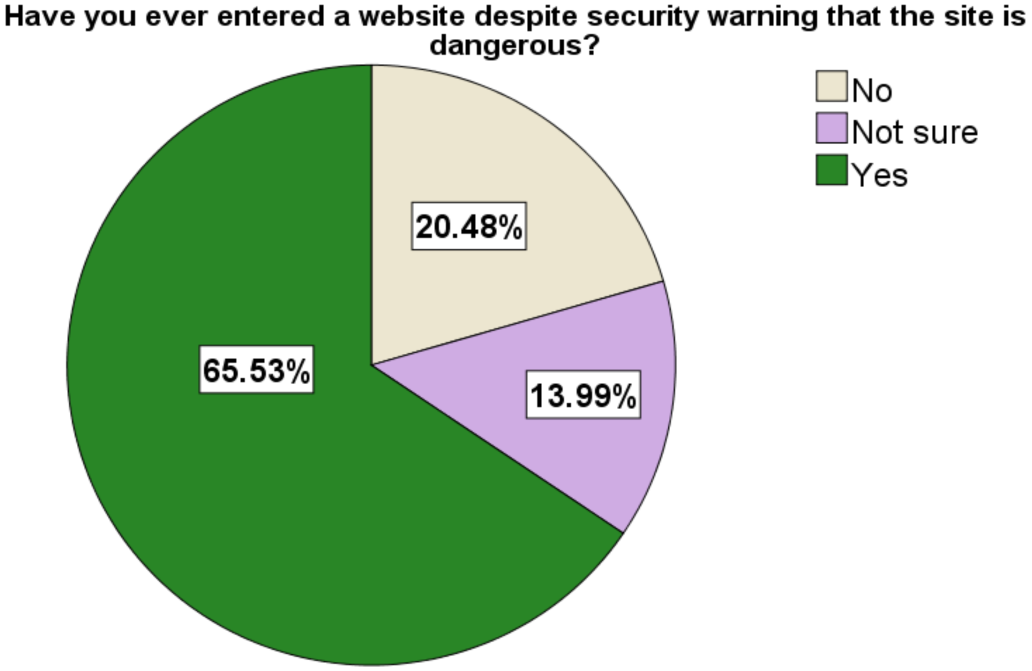

Figure 10: Participants concerned about entering the site despite security warnings

4.3 Awareness Level

The awareness level is measured concerning the selected privacy and security questions from which the null hypotheses were derived as analyzed in the previous section. For each of the hypotheses (questions considered), there are safe and unsafe parameters as illustrated in Table 3.

Table 3. Considered parameters for each hypothesis (question)

Hypothesis	Safe parameter	Unsafe parameter
H01.	Yes	No
H02	No	Yes
H03	Yes	No
H04	Yes	No
H05	Concerned	Not concerned
H06	Yes	No
H07	Yes	No
H08	Yes	No
H09	Yes	No
H010	No	Yes

Applying the analysis of the hypotheses shown in Table 3 on equation (1) leveraging the existing models [26], [27]. The equation calculates the awareness level in a range of 0 to 1 which is converted to percentage as displayed in Figure 11.

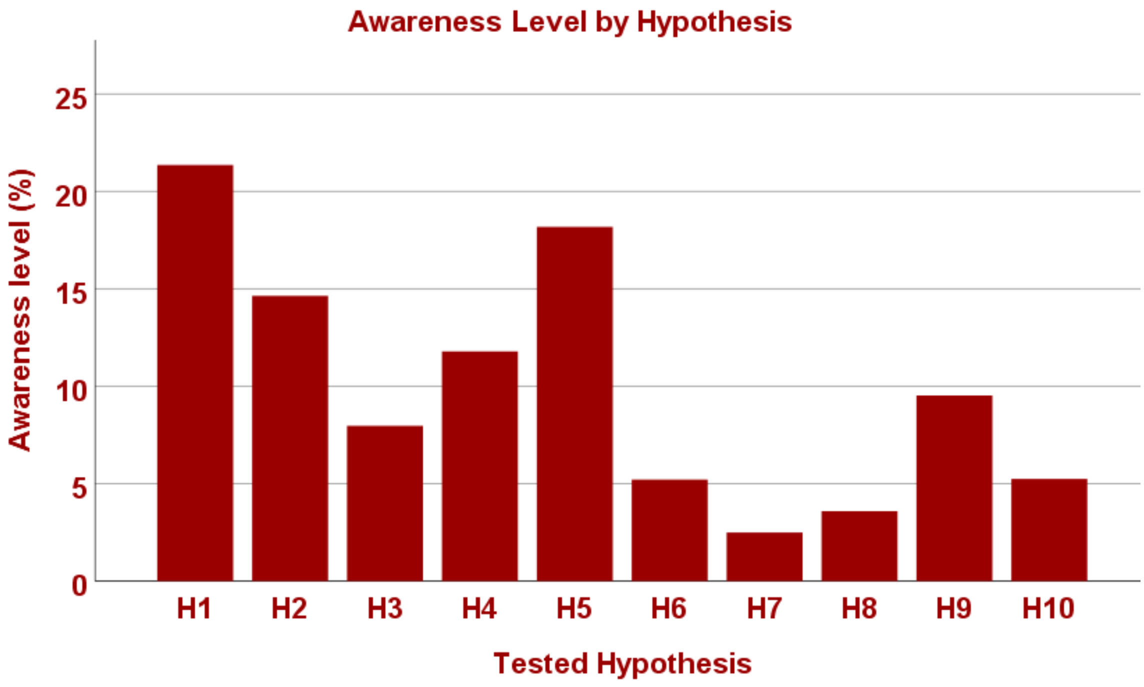

Figure 11: Percentage AL of the Hypothesis

5. FINDINGS

Identifying and avoiding scams is an essential attitude to hold high. The understanding or knowledge of being able to identify and forestall such risks is what this study has investigated in Nigeria presently. Nigerians are quite aware of some basic privacy and security issues as stated in [18]. However, on average, it has been found using equation (1) that only about 21.36 % of the respondents are aware of and use the screen lock mechanism to secure their Smartphones. Also, 7.97 % of the respondents agreed to have enabled 2FA authentication to secure their devices. Similarly, 3.59 % of the respondents are aware of the danger of self-disclosure of personal data. On permission requests, it is observed that only 5.21 % of respondents review the privacy policy before granting App permission. Over 9.53 % are aware of the potential danger of using public Wi-Fi Networks.

From the quantitative analysis, some respondents admitted being aware of security settings on their smartphones and do activate screen locks. Other participants also indicated that they are aware of what 2FA is and how it works. Several users also agreed to have disclosed their data or credentials on various platforms. Similarly, some participants said they do review the application’s privacy policies before granting permission requests for applications to run on their devices. On the use of public networks (Wi-Fi), some of the respondents acknowledged their awareness of the associated risks of using public Wi-Fi.

Although a significant percentage of participants are aware of background data collection by applications. A large number lack awareness of how to access and manage privacy settings effectively. Equally important, while some smartphone users are aware of the screen lock mechanism, a good number of the respondents are not aware, ignore or are ignorant of its importance. On the 2FA verification technique, though a certain percentage of the respondents acknowledged their familiarity with it. However, a considerable are completely ignorant of 2FA security measures.

6. CONCLUSIONS

This survey aims to divulge the awareness level of smartphone users concerning privacy and security threats. Findings revealed the areas with laudable awareness and significant loopholes requiring urgent consideration. The inferences of these discoveries highlight the need for active procedures to improve awareness and empower smartphone users to make informed decisions about their data privacy. Quantitively, the survey indicated a substantial percentage of respondents who are cognizant of the fact that smartphone apps collect personal data, reflecting an increasing consciousness about data practices in the digital age. However, the limited understanding of background data collection and data sharing with third-party companies signifies the need for comprehensive education campaigns to bridge these knowledge gaps. Concerns expressed by a majority of participants regarding unauthorized access to personal data and data breaches underscore the gravity of the issue. The willingness of respondents to review app permissions, although not universally practised, indicates a potential willingness among users to engage in privacy-enhancing behaviours if provided with clearer guidance and more intuitive interfaces. Online resources emerged as a key source of information for users seeking to educate themselves about privacy practices. However, the complexity of privacy policies and the challenge of interpreting domain knowledge present an obstacle that requires attention. Developing user-friendly resources, such as interactive guides and easily comprehensible privacy policies, can facilitate a better understanding of data practices and engender a sense of control among users. While there is a foundation of awareness among smartphone users regarding online privacy and data security as asserted by [17]. There is ample room for improvement. Future efforts should focus on streamlining privacy settings, enhancing transparency in data collection and sharing practices, and providing accessible educational materials. By empowering smartphone users with the knowledge and tools to safeguard their data, we can collectively create a more privacy-conscious digital landscape and foster a sense of agency in an increasingly data-driven world. As technology continues to advance and data security becomes a major concern. Constant research and collaborative initiatives among stakeholders, users, app developers, policymakers, and educators are essential in fostering a culture of privacy and security awareness practices.

7. REFERENCES

[1] T. Jabar and M. M. Singh, “Exploration of Mobile Device Behavior for Mitigating Advanced Persistent Threats (APT): A Systematic Literature Review and Conceptual Framework,” *Sensors*, vol. 22, no. 13, pp. 1–38, 2022, doi: 10.3390/s22134662.

[2] Z. Shouran, A. Ashari, and K. T. Priyambodo, “Internet of Things (IoT) of Smart Home: Privacy and Security,” *Int. J. Comput. Appl.*, vol. 182, no. 39, pp. 3–8, 2019, doi: 10.5120/ijca2019918450.

[3] NCC, “Nigerian Communications Commission,” 2023. https://ncc.gov.ng/statistics-reports/reports-publications (accessed Aug. 07, 2023).

[4] P. Taylor, “Smartphone mobile network subscriptions worldwide,” 2023. https://www.statista.com/statistics/330695/number-of smartphone-users-worldwide/ (accessed Aug. 07, 2023).

[5] S. C. Kishore *et al.*, “Smartphone-Operated Wireless Chemical Sensors: A Review,” *Chemosensors*, vol. 10, no. 2, pp. 1–22, 2022, doi: 10.3390/chemosensors10020055.

[6] A. S. Rather and M. Khazer, “Impact of smartphones on young generation,” *Libr. Philos. Pract.*, vol. 2019, 2019.

[7] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, “Digital identities and verifiable credentials,” *Bus. \& Inf. Syst. Eng.*, vol. 63, no. 5, pp. 603–613, 2021.

[8] J. Abah, O. V Waziri, M. B. Abdullahi, U. A. Ume, and O. S. Adewale, “Extracting Android Applications Data for Anomaly-based Malware Detection,” *Glob. J. Comput. Sci. Technol. Vol.*, vol. 15, no. 5, pp. 0–8, 2015.

[9] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, “A Usability Study of Five Two-Factor Authentication Methods,” *usenix Conf.*, pp. 357–370, 2019.

[10] A. Jegede, G. Odii, M. Magaji, and G. Aimufua, “Assessment of Security Awareness Level of Mobile Device Users in Tertiary Institutions in Plateau State of Nigeria,” *J. Adv. Comput. Technol. Appl.*, vol. 3, no. 2, pp. 1–8, 2021, [Online]. Available: https://www.researchgate.net/publication/357407107%0AAssessment

[11] R. Palanisamy, A. A. Norman, and M. L. Kiah, “BYOD Policy Compliance: Risks and Strategies in Organizations,” *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 61–72, 2020, doi: 10.1080/08874417.2019.1703225.

[12] M. Talal *et al.*, *Comprehensive review and analysis of anti-malware apps for smartphones*, vol. 72, no. 2. Springer US, 2019. doi: 10.1007/s11235-019-00575-7.

[13] P. Nagarjun and S. S. Ahamad, “Review of Mobile Security Problems and Defensive Methods,” *Int. J. Appl. Eng. Res.*, vol. 13, no. 12, pp. 10256–10259, 2018.

[14] I. Almomani and A. Al Khayer, “A Comprehensive Analysis of the Android Permissions System,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3041432.

[15] C. I. Eke and A. N. Anir, “Bring your own device (byod) security threats and mitigation mechanisms: Systematic mapping,” in *2021 International Conference on Computer Science and Engineering (IC2SE)*, 2021, vol. 1, pp. 1–10.

[16] F. O. Nzeakor, N. B. Nwokeoma, and P.-J. Ezeh, “Pattern of Cybercrime Awareness in Imo State , Nigeria : An Empirical Assessment,” vol. 14, no. June, pp. 283–299, 2020, doi: 10.5281/zenodo.3753223.

[17] J. A. Odey, I. Agbonlahor, and A. Prince, “A SURVEY ON THE PERCEPTIONS AND AWARENESS OF CYBER SECURITY IN NIGERIA,” 2021. [Online]. Available: https://www.researchgate.net/publication/357000811%0

AA

[18] A. A. Garba, M. M. Siraj, and S. H. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 1, pp. 572–584, 2022, doi: 10.11591/ijece.v12i1.pp572-584.

[19] J. Abah, A. E. Chahari, E. A. Samuel, and E. P. Musa, "Behaviour-Based Detection: An Approach for Securing Android Systems Against Zero-Day Malware Attacks," *FUDMA J. Sci.*, vol. 4, no. 3, pp. 266 –275, 2019, [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[20] M. Koyuncu and T. Pusatli, "Security Awareness Level of Smartphone Users : An Exploratory Case Study," vol. 2019, 2019.

[21] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt, "A survey on smartphone user's security choices, awareness and education," *Comput. Secur.*, vol. 88, p. 101647, 2020, doi: 10.1016/j.cose.2019.101647.

[22] M. Amin *et al.*, "Security and privacy awareness of smartphone users in Indonesia," in *Journal of Physics: Conference Series*, 2021, vol. 1882, no. 1. doi: 10.1088/1742-6596/1882/1/012134.

[23] T. Moletsane and P. Tsibolane, "Mobile Information Security Awareness Among Students in Higher Education," *2020 Conf. Inf. Commun. Technol. Soc. ICTAS 2020 - Proc.*, pp. 1–6, 2020, doi: 10.1109/ICTAS47918.2020.233978.

[24] P. Shah and A. Agarwal, "Cybersecurity behaviour of smartphone users in India: an empirical analysis," *Inf. Comput. Secur.*, vol. 28, no. 2, pp. 293–318, 2020, doi: 10.1108/ICS-04-2019-0041.

[25] A. Chin, B. Jones, and P. Little, "A Comparative Analysis of Smartphone Security Behaviors and Practices," vol. 17, no. 3, pp. 57–80, 2021.

[26] M. Amin *et al.*, "Security and privacy awareness of smartphone users in Indonesia," *J. Phys. Conf. Ser.*, vol. 1882, no. 2021, 2020, doi: 10.1088/1742-6596/1882/1/012134.

[27] M. N. Y. Ali, M. L. Rahman, and I. Jahan, "Security and privacy awareness: A survey for smartphone user," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 483–488, 2019, doi: 10.14569/ijacsa.2019.0100964.