https://research.lukenyauniversity.ac.ke/

ISSN 2663-3183 MULTIDISCIPLINARY JOURNAL (LUMJ)

Vol 1, p.215-225

RELATIONSHIP BETWEEN THE BEHAVIOR OF KENYAN SMARTPHONE USERS AND AWARENESS OF INFORMATION SECURITY PRACTICES

Kosgey L.*[1], Mbogo C.[2], Munene D.[3]

Kenya Methodist University*[1, 2, 3]

Corresponding author: kosgeylynet@gmail.com*1 https://orcid.org/0000-0001-8209-3017

Article history
Received: August 19, 2019
Received in revised form: August 29, 2020
Accepted: November 23, 2020
Available online: https://www.lukenyauniversity/research/

ABSTRACT

People are becoming increasingly dependable on their phones to accomplish day to day activities, such as getting information and money transfer. Yet, smartphones hold a lot of personal information that can cause tremendous effect on user privacy and security, if exposed. Consequently, there is a need to understand users' awareness and behavior when using their mobile phones. Unfortunately, most smartphone users in Kenya lack a proper mobile awareness model which can be used to raise and maintain awareness about information security. This study explored the awareness level of 393 Kenyan smartphone users on information security threats that face them and the behavioural choices that leaves them vulnerable. An online structured survey was used to investigate the relationship between the behavior of Kenyan smartphone users and awareness of information security practices. The results showed that users are aware of smartphone threats yet they continue to make wrong choices that leaves them vulnerable to attacks. An awareness model might improve security awareness and hence reduce the amount of risk associated with use of smartphones.

Keywords: Information Security, Users, Threats, Behavioral Awareness.

1. INTRODUCTION

Seventy five percent of mobile transactions in Kenya happen through mobile phones (Communications Authority of Kenya, 2018). In addition, the rise in the youth population of Kenya with a higher purchasing power has a great impact on the number of smartphones they purchase. The high purchasing power has also contributed to a tremendous reduction in the cost of the gadget (Jumia, 2019). Also, three quarters of the population are under the age of 30 hence they are deemed

comfortable utilizing all the features in smartphones.

The high proliferation of smartphones means that many mobile phone users may be at risk of various attacks and prone to misuse of these communication gadgets, which may affect their privacy and security. For example, the cost of cybercrime in 2017 through mobile use was 25 Million Kenya Shillings (Serianu, 2017). Such examples of attacks may be because the amount of personal data, sensitive documents, and credentials stored and processed by smartphones makes them an appealing target for attackers.

Unfortunately, recent research also shows that the lack of privacy and security on mobile phones is caused by lack of user awareness (Androulidakis, 2016). Further, the study also shows that mobile phone users tend to assure themselves that mobile phones are secure, and therefore are less cautious about the security practices that they should take (Androulidakis, 2016). In addition, research has shown a rise in the reported cases in Kenya to the police, on cybercrime and cyberattacks (Cyber & Report, 2018). This may imply that security awareness among Kenyan technology users is still low and hence they become easy targets for hackers. Also, a study carried out among 281 students of Slovenian faculties, investigating threat perception on mobile devices (Markelj & Bernik, 2015), showed that the sample student population had a low awareness of security threats and security measures, and the authors suggest that education and awareness levels must be increased in Slovenia to counter this development. Therefore, for mobile phone users to better protect themselves, there may be a need for increased awareness of potential risks that are associated with smartphone use. Consequently, user awareness may improve privacy and security among Kenyan smartphone users.

This paper presents research conducted to investigate the relationship between the behavior of users while utilizing mobile phones and their awareness of information security practices.

The paper is divided into six sections. Section two discusses the related work and Section three presents the theory that underpins this research. Section four illustrates the methodology used, and Section five presents the results and discussion. The paper concludes with recommendations and acknowledgement.

2.0 RELATED WORK

Previous research has been done on how smartphone users security and privacy-related decisions are influenced by their attitudes, perceptions, and understanding of various security threats (Alsaleh, Alomar, & Alarifi, 2017). Further, smartphone users who download apps tend to be unaware of security risks associated with downloading from online repositories (Mylonas, Kastania, & Gritzalis, 2013). Users believed that the controlled app market, for example Google Play, is secure (Mylonas et al., 2013).

To understand if users are concerned about their security threats, a survey revealed that a high percentage, over 65% of smartphone users, are concerned about their privacy and security although they continue practicing risky activities like giving application permission to access their data (Symantec Corporation, 2015). This is further pointed out among Middle East smartphone users who need urgent measures to improve their security practices (Das & Khan, 2016).

Despite the numerous studies showing that users do not have good security awareness, some research has proved otherwise by showing different results when research subjects and environment varies. For instance, a study to show security awareness and adoption of security controls by smartphone users, found that university students in Rutgers, United States, are aware of risk in smartphones and have adopted authentication controls like anti-theft control (Parker, Ophoff, Van Belle, & Karia, 2016) .This means

knowledge awareness varies with subjects and environment. The results explain why there is cybercrime in Africa that taps into a low awareness population that saw five East African countries lose 245 Million dollars to online fraud (Osborn Quarshie & Martin- Odoom, 2012). In addition, cyber security is listed as an emerging threat in Kenyan national security (Kiboi, 2015). Therefore, there is a need to understand the behavior of smartphone users versus the awareness level while they use mobile phones. This research addresses this need, specifically for mobile phone users in Kenya.

3.0 THEORETICAL FRAMEWORKS

Theorizing is a process containing assumptions, accepted principles, and rules of procedures to explain or predict the behavior of a specified set of phenomena (E. Weick, 1995). Protection motivation theory (PMT) and Unified theory of acceptance and use of technology (UTAUT), underpin this work.

PMT predicts how people cope with and make decisions to protect themselves after receiving fear-arousing recommendations. It suggests that when faced with a threat people react in two assessment processes, one is focused on the threat itself and another the knowledge to act against the threat. It is mainly used to explain decisions behind threats. The theory has been widely used in
Cybersecurity in designing of nudges to improve online behaviors (van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019), online virus protection behavior (Lee, Larose, & Rifon, 2008), information privacy concerns on social networks (Adhikari & Panda, 2018) and security activity among users who know to protect organizations systems but fails to do so (Workman, Bommer, & Straub, 2008).

UTAUT seeks to explain user intentions to use information systems and later used to explain usage behavior (Venkatesh, Morris, Davis, & Davis, 2003). UTAUT identifies four key factors which are: performance expectancy, effort expectancy, social influence, and facilitating conditions. It also identifies four moderators: age, gender, experience, and voluntariness related to predicting behavioral intention to use a technology and actual technology used. This theory gives us more insight on behavioural intentions of smartphone users.

UTAUT contributes in refining current context effect-legacy system habit to feature-level use. It has also contributed on adding a library of focal events that can be remembered, for example, to rate job performance (Viswanath Venkatesh et al., 2016). This theory explains the choices the user makes in using their smartphones.

UTAUT has contributed in this research to explain how users interact with their phones and explain some user choices. Whereas, PMT explained user choices when they understand they are faced with security threats.

1.0 STUDY METHODOLOGY

1.1 Metric of research

Participants were chosen from an urban and rural background to eliminate any bias on awareness due to their level of exposure based on geographical location.

To understand user awareness on information security practices, the research investigated the following: (i) awareness about the access of private data on smartphones; (ii) Security measures used on their phones; (iii) Threat awareness

To understand users' level of awareness we asked questions to know if they are aware that some applications require users to allow them to access private data on their phones, such as contacts, photos, location and device information.

To also investigate security measures on users' phone, we asked questions like listing the security features they use. We also asked whether they have installed antivirus, this is to further understand their behavior. UTAUT contributes in explaining users' choices as it explains their behavior basing it on the security choices.

Lastly, we examined whether they are aware of threats on their phones. Questions on common threats were asked to determine awareness level. This question is such as, if they are aware that phone updates improve security.

1.2 Participants

In order to investigate the relationship between the behavior of Kenyan smartphone users and awareness of information security practices, an online structured questionnaire was used and some questionnaires printed. To calculate the sample size, we considered the total population of Nairobi and Eldoret cities, estimated at 3 million people. To calculate the sample size, we used the formula below;

$$\text{Finite population: } n' = \frac{n}{1+\frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2 N}}$$

where
z is the z score
ε is the margin of error
N is population size
p̂ is the population proportion

This is considering a confidence interval of 95%. Where z or 95% confidence level is 1.96 and population proportion of 0.5. The sample size was to be at least 384 random smartphone users to reduce bias. However, the final number of participants was 430.

The demographics are as shown in Table 1. According to the Table, there were almost a 50-50 representation of male and female. The age group with a higher representation was between the age of 20 and 30 at 53 percent, followed by 30-40 years with a percentage of 30 percent. Additionally, 71 percent of the sample were working or self-employed with 18 percent as students. The participants also used android smartphones and displayed moderate to excellent IT knowledge with only 3 percent without IT knowledge. Finally, the majority of the participants lived in urban areas and from Kenya.

4.0 Data Collection

An online questionnaire was chosen as it allows questions preview before sharing, collecting of data in Google Spreadsheets, provides a friendly interface, and can be used to reach many respondents irrespective of their geographical location. The questionnaire was designed using Google forms and consisted of two parts: (i) demography; and (ii) User Awareness on information security practices. Offline questionnaires were also utilized where the questions were printed for any user who had no access to the Internet. Participation in the research was open to users of any mobile operating system.

In this study, to alleviate any potentially ambiguous questions, a pilot survey was sent out to 20 individuals. This process was important to solicit feedback and ensure that respondents would not have problems in answering the questions and eliminate ambiguity.

A total of 520 questionnaires were sent out by sharing a Google form link via email, WhatsApp, and printing the form. Of the 520 questionnaires sent out, 430 smartphone users responded. This represents an 83% response rate.

The survey contained questions categorized into two sections; the first section was on user demographics that asked user gender, age group,

profession, IT Knowledge and the type of setting they live in. The second sections on user awareness included; firstly, gaining insights on the type of smartphone the user owned. Secondly, what they used their smartphones for and what type of data they stored on it. Thirdly, knowing where the user downloaded applications from and the factors they would consider when installing an application and finally, whether they believed applications they downloaded underwent a prior security review.

4.1 Data Analysis

The data collected using the forms was converted to a spreadsheet. The data was then cleaned using Microsoft Excel. Data cleaning involved identifying and correcting the inaccurate record. The data contained a mixture of qualitative and quantitative research. Analysis of 91 percent (393 Users) of the population, who were Kenyans was performed. Data was then represented through text, graphs and in tabular format.

In this study security threat awareness acts as an independent variable while user behavior is the dependent variable.

5.0 RESULTS AND DISCUSSION

The results considered 393 users, who form 91 percent of the population as per table 1 below.

5.1 User Awareness

Outlined in Figure 1 below, the findings infer that almost all users are aware that some applications require them to allow access to private data. This finding may explain why most of the users erase their phones when handing it over to the next user and have also set a pin or password on their phones. Moreover, users also update their phones regularly, and they tend not to click on any link or QR code that they receive.

Conversely, the same users tend to forget to disable GPS after use. This might be because most users in this research use android phones, where users don't have options on the use of GPS. Apple for example, have options of reminding users the applications using locational

Table 1: Smartphone users Demographics

Characteristics	Category	Overall	Percen
Gender	Male	223	
	Female	198	
	Prefer not to answer	8	
	Not responded	1	
Age Group	Less than 20 years	4	
	20-30 years	229	
	30-40 years	130	
	40-50 years	39	
	Above 50 years	16	
	Prefer not to answer	11	
	Not responded	1	
Profession	Working/Self Employed	305	
	Student	78	
	Retired	1	
	Unemployed	37	
	No answer	9	
Phone Operating System	Android by Google	374	
	IOS by Apple	38	
	BlackBerry	2	
	Windows Phone	3	
	I am not Aware	5	
	Not responded	8	
Phone Monitored by employer	Yes	20	
	No	372	
	Not responded	1	
IT Knowledge	Good	97	
	Moderate	173	
	EDxocne'tl lehnatve IT	144	
	knowledge	12	
	Not responded	4	
Settlement Setting	Rural	53	
	Urban	372	
	Not responded	5	
Country	Kenya	393	
	Outside Kenya	31	
	Not responded	0	
Smartphone Ownership	Yes	429	1
	No	1	

services and if they want to disable them (Apple Inc., 2018).They also have the option of only allowing locational services while the app is in use.

Figure 2 depicts that approximately half of the users lock their phones using password, pin or fingerprint, update their phones and back-up their phone data. However, more than half of the users do not use

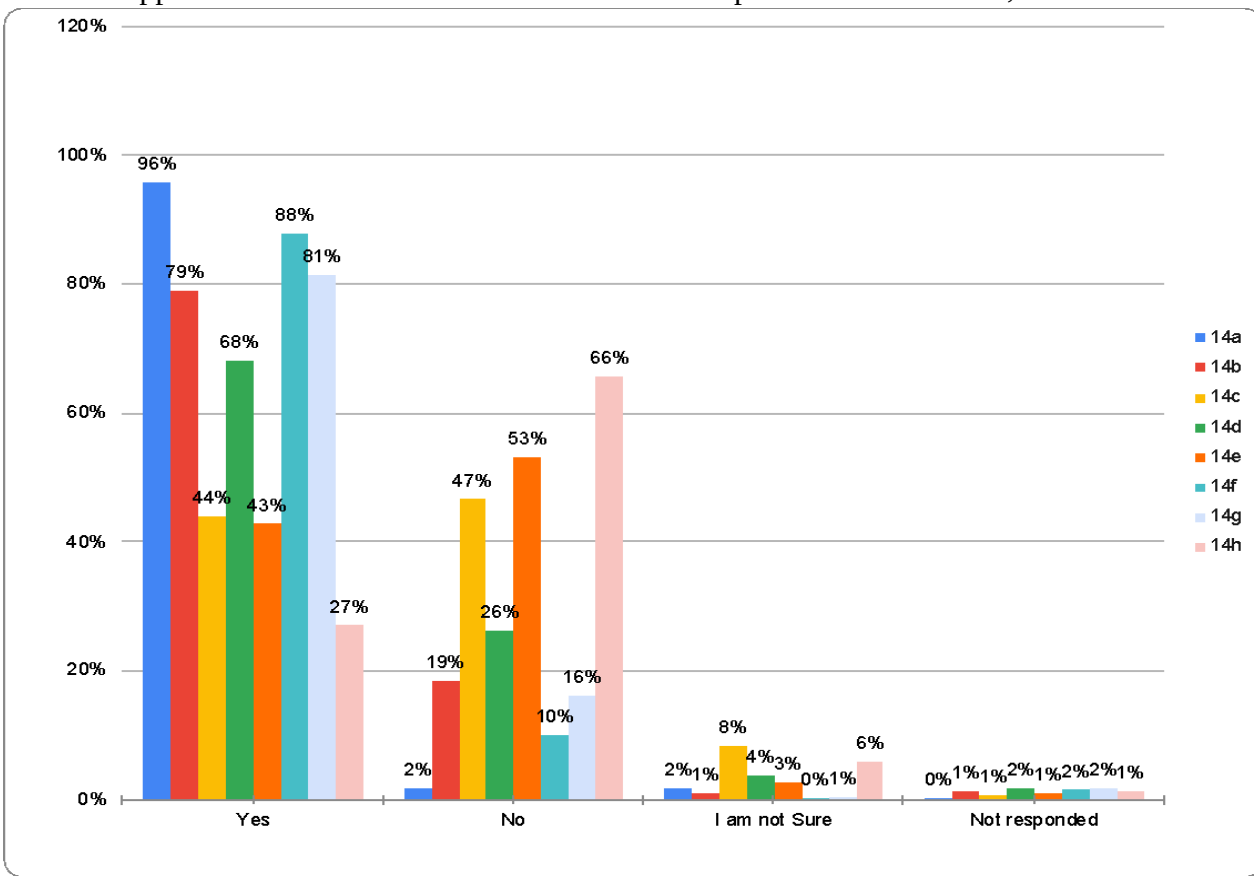

Figure 1 An illustration of User Threat Awareness

Where the following numbers stand for;

14a, Are you aware that some applications require you to allow them to access private data on your smartphone, such as, contacts, photos, location, device information and more 14b, Do you sometimes forget to disable locational service GPS, on your phone after use? 14c, Do you know/have stored your smartphones IMEI (International Mobile Equipment Identity) number? 14d, Do you erase your smartphone before you give it to the next user?

14e, Do you sometimes connect to public WIFI when performing transactions?

14f, Have you set a pin, password or any physical control on your phone?

14g, Do you update your phone and mobile applications regularly?

14h, Do you click on any link or scan QR code shared?

Additionally, users tend to connect to public WiFi when performing bank transactions which may expose them to hackers. This can mean that users trust public connection. Finally, these users don't have their phone IMEI number. IMEI number assist in tracing a mobile identity and hence can be used to locate a lost phone.

Antivirus neither nor do they encrypt their phone data. This may infer that password and pin use is the best practice they have learned through an incidence experienced such as data loss or unauthorized access of their mobile phone.

5.2 Security Measures on Phones

This may also be because, we use pin or password often in our daily lives like in the bank, emails and mobile service providers. These entities remind us often of putting these measures either through social media, radio or TV. That means if people get information constantly, they change their habits. In Brazil for instance, to control population the government through media exposed societies to soap operas specifically of families with few children. Admittedly, the fertility rates declined (Ferrara, Chong, & Duryea, 2012).

Also, users utilize public WiFi, are unaware of phone scam or suspicious contents, and have active locational services and install untrusted applications. This might mean that they are less aware of these media of data loss or have never experienced data loss through these means. This gap can be bridged by training as suggested by a user "Information Security lessons should be introduced to everyone at their early life so they can grow into it. This will reduce rates of data privacy violations."

5.2.1 Antivirus Installation and Use

We can interpret from Figure 3 and 4 that most smartphone users do not install antivirus on their phones and instead install it on their Personal Computers or Laptops. This might mean that users think that laptops are more vulnerable to attacks than smartphones or that PCs need more protection than mobile phone

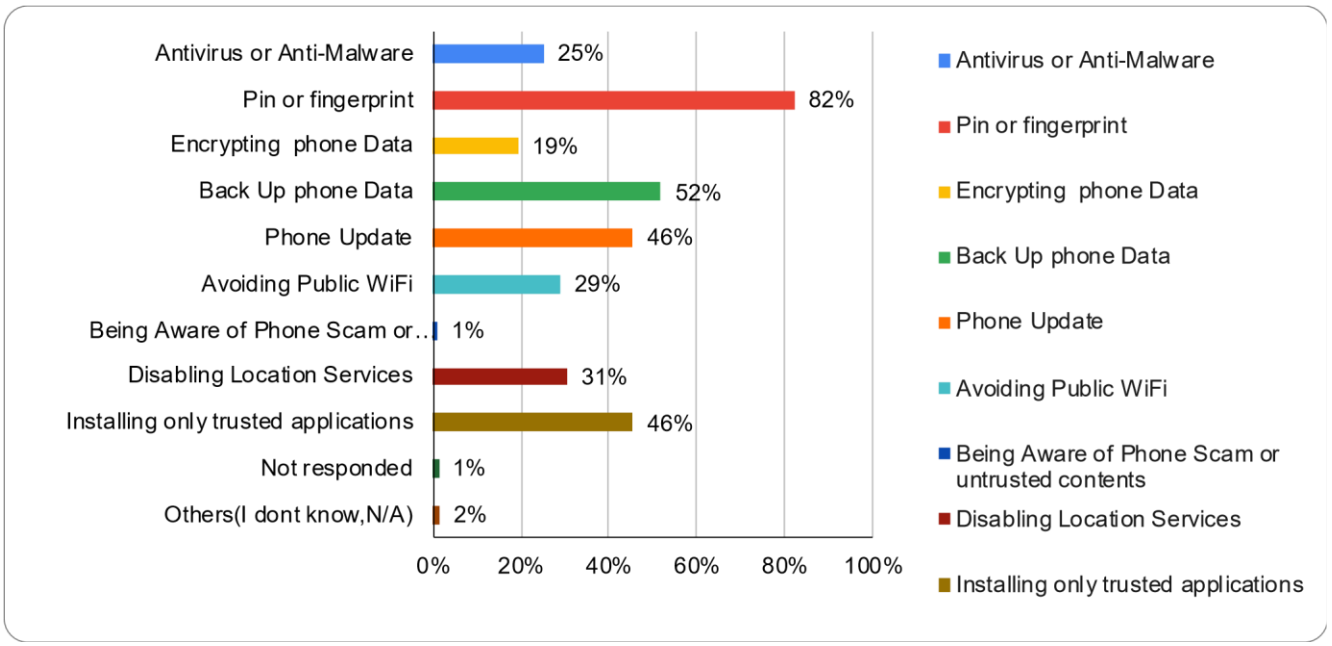

Figure 2: An illustration of security features utilization on user smartphones

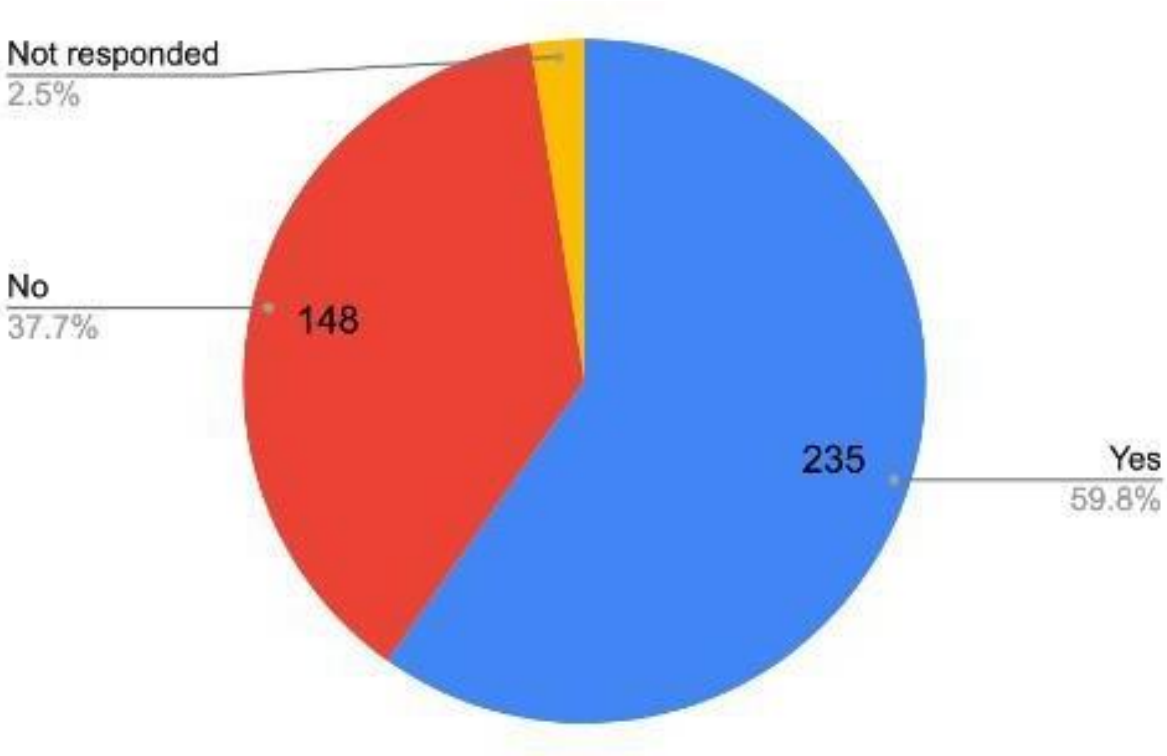

Figure 3: An illustration of Importance of Antivirus

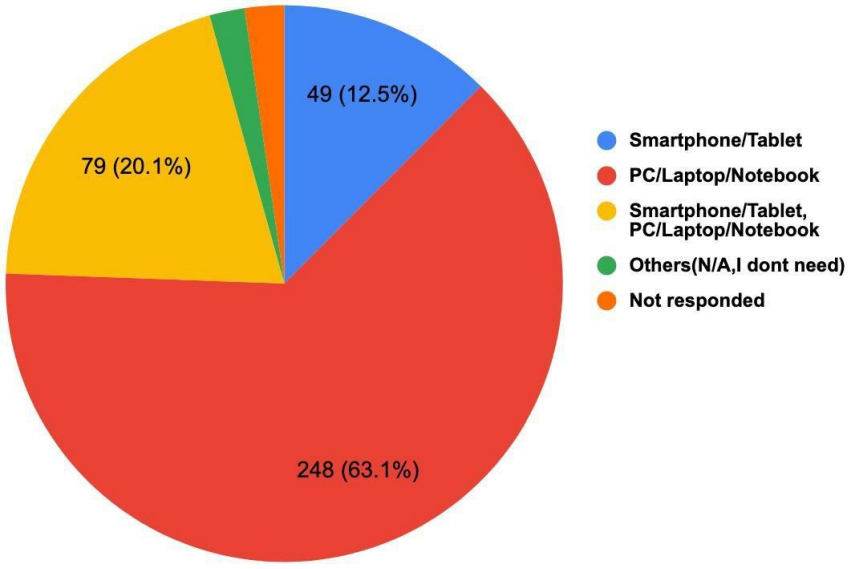

Figure 4: An illustration of Antivirus Installation on Various Gadgets

5.3 Awareness on Potential Threat

Figure 5 below shows that a high number of users are aware that;

i. Applications updates improves phone security.
ii. They are aware that some links shared or QR codes to scan are not legitimate.
iii. Applications may contain spyware that can access private information on smartphone.
iv. Some banking application pose as legitimate but instead steal banking information.
v. Smartphone sensitive data can be transferred to a new user.
vi. Smartphone connected to open public WiFi hotspots hence exposing personal and financial data.

5.0 CONCLUSION AND RECOMMENDATIONS

Smartphone users are aware of security threats facing them, although they still make choices that make them vulnerable. This might show that users leave security responsibilities to other institutions like the owners of smartphone applications for example a bank, which compensates in case of breach, or the creator of applications. Or worse, they are aware and just do not care much unless these applications force them to access some of personal resources on the phone. This might also mean that some users are aware and that they need constant reminders.

These findings show that awareness level is high as most users are aware of common security risks. Users are generally aware of most potential threats to their phones. Hence there is an awareness gap on smartphone users' action rather than knowledge. For example, users are aware that open public WiFi is risky, yet they still connect to it.

The recommendation is that applications be regulated and apps be ranked on the basis of user security. In addition, software developers develop more apps where by default the

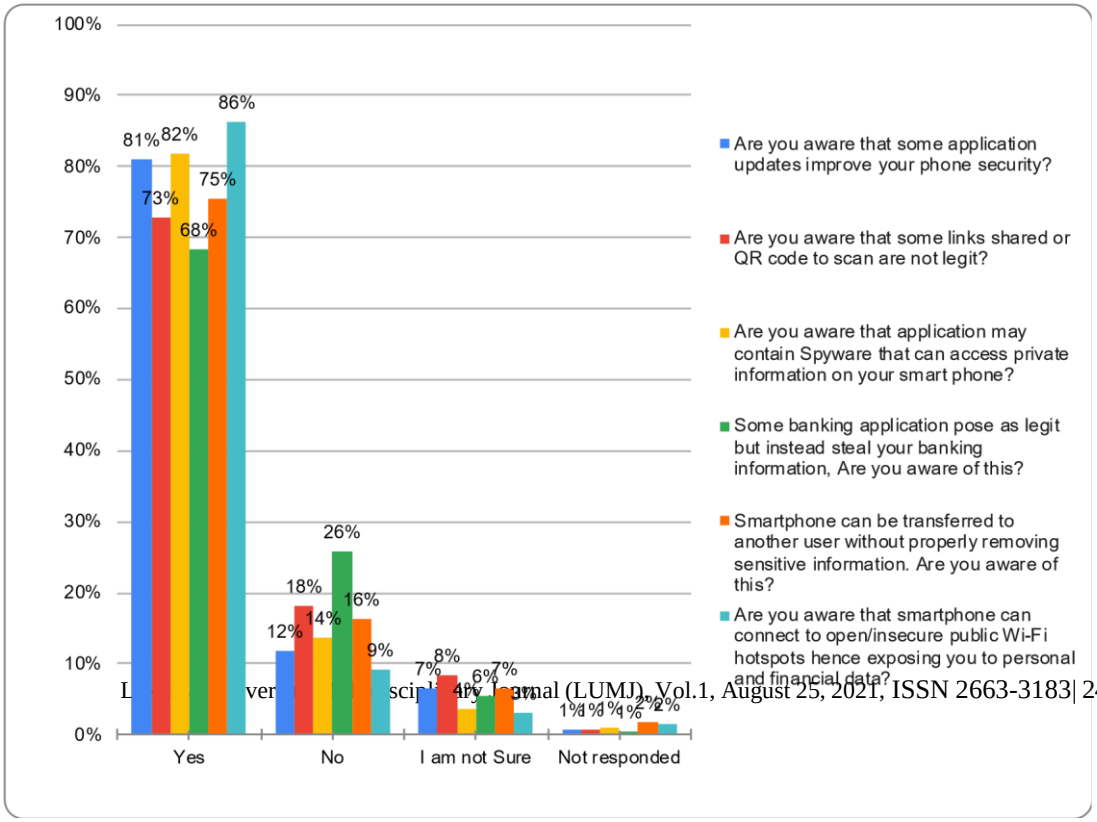

Figure 5: An illustration of Awareness of consequences on potential Threats

user data is protected. As a user suggested "You help us to protect our privacy".

For security awareness to be fully accomplished, having discovered that Kenyan mobile users are knowledgeable on user security, future work will need to come up with a model that addresses the gap identified in this research. The gap being user behavior depicted by their actions and also, to address user attitude on mobile security. This is because information security awareness model on an individual should be based on three dimensions, namely knowledge (what users know), attitude (what users think or feel) and behavior (what users do) (Kruger & Kearney, 2006).

Finally, the future work of this research would be to design a model addressing the knowledge gaps in information security awareness among smartphone users identified on this research. Future work on this study will study user perceived risk level and the countermeasures that can be used to protect smartphone users.

1.0 ACKNOWLEDGEMENTS

We would like to thank Kenya Methodist university of supporting this research and Lukenya University for sponsoring the publishing of this paper.

REFERENCES

Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and *Quarterly*. https://doi.org/10.1086/250095

Ferrara, E. La, Chong, A., & Duryea, S. (2012). Soap Operas and Fertility: Evidence from Brazil. *SSRN Electronic Journal*, (June). https://doi.org/10.2139/ssrn.1820921

Jumia. (2019). *Kenya Mobile Report 2019*.

Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing*, *31*(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*. https://doi.org/10.1371/journal.pone.0173284

Androulidakis, I. I. (2016). *Mobile phone security and forensics: A practical approach, second edition. Mobile Phone Security and Forensics: A Practical Approach, Second Edition*. https://doi.org/10.1007/978-3-319-29742-2

Apple Inc. (2018). iOS Security iOS 12. *White Paper*.

Communications Authority of Kenya. (2018). Fourth Quarter Sector Statistics Report for the Financial Year 2017/2018 (April-June 2018), *2018*(June), 35 p.

Cyber, A., & Report, S. (2018). *Cyber Security Skills Gap*.

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*. https://doi.org/10.1108/ICS-04-2015-0018

E. Weick, K. (1995). What theory is not, theorizing is. *Administrative Science*

Kiboi, N. (2015). *Cyber Security as an Emerging Threat to Kenya Security*.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296.

https://doi.org/10.1016/j.cose.2006.02
.008

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454. https://doi.org/10.1080/01449290600 879344

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications.* https://doi.org/10.1016/j.jisa.2014.11. 001

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers and Security*. https://doi.org/10.1016/j.cose.2012.11
.004

Osborn Quarshie, H., & Martin- Odoom, A. (2012). Fighting Cybercrime in Africa. *Computer Science and*
Engineering. https://doi.org/10.5923/j.computer.20 120206.03

Parker, F., Ophoff, J., Van Belle, J. P., & Karia, R. (2016). Security awareness and adoption of security controls by smartphone users. In *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec2015*. https://doi.org/10.1109/InfoSec.2015. 7435513

Serianu. (2017). *Demystifying Africa's Cyber Security Poverty Line*.

Symantec Corporation. (2015). Internet Security Threat Report 2015. *Internet Security Threat Report*.

https://doi.org/10.1007/s10207-0140262-9 van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection