

**DIGITAL STORYTELLING FOR INCREASING INFORMATION
SECURITY AWARENESS AMONG KENYAN SMARTPHONE USERS: A
CASE STUDY OF NAIROBI AND ELDORET**


LYNET JESANG KOSGEY

A Thesis Submitted to the School of Science and Technology in Partial Fulfillment
for the requirements of the degree of Master of Science in Computer Information
Systems, Kenya Methodist University

November, 2020

DECLARATION

This thesis is my original work and has not been presented for a degree or any other award in any other University

Signed:  Date: ...17th August 2020...

Lynet Jesang Kosgey

CIS-3-2235-1/2016

We confirm that the work reported in this thesis was carried out by the candidate under our supervision.

1. Signed: Date:

DR. CHAO MBOGO

2. Signed: Date:

DAVID MUNENE

COPYRIGHT

© Lynet Kosgey. All rights reserved. No part of this thesis may be reproduced, stored in any retrieval system or transmitted in any form or by any means, electronically, mechanically, by photocopying or otherwise, without prior written permission of the author or Kenya Methodist University, on that behalf

DEDICATION

This research is devoted to:

KAPBARAKA FAMILY

for raising me to believe that anything was possible

MY DAUGHTER NATALIE

Who is my reason for being.

ACKNOWLEDGEMENT

This research has been accomplished with contribution and support from a multitude that I am deeply indebted.

I am forever grateful to Dr. Chao Mbogo, for her close supervision, mentorship, support, affirmation and guidance throughout the research process.

To my second supervisor Mr. David Munene, for your patience and recommendations which revamp this thesis and keeping me focused.

I am also grateful to my readers Janet, Nelly, Anthony and Hellen. Thank you for your positive critique and motivation to write better.

I would like to thank my friends, colleagues and classmates who encouraged me in the process; Justina, Nelly, Doris, Maggy, Rozy, Isaac, Purity, Kibe, Kibii, Edwin, Sunil, Victor, Olivier, Denis, Kosgey, Chandra, Fr. Isaiah, Fr. Ouma, KamiLimu group and Mwaniki for helping in video production. You each have been a source of inspiration and courage.

For the support and encouragement from my family throughout - thank you for believing in me. Last but not least, praise be to God, for sustenance and providence.

ABSTRACT

The rapid increase of smartphone proliferation in Kenya has resulted in users being dependent on their phones for everyday activities. This increased interaction with smartphones has posed a significant threat to users' privacy and security. The exposure to threats demonstrates a need to understand users' security awareness and behavior when using their mobile phones. Therefore, this study sought to establish the level of security risk awareness and user behaviour among smartphone users in Kenya, in order to design a customized security awareness model with the aim of reducing information security risks. The specific objectives include: to investigate information security-related behavior among Kenyan smartphone users, and to design and evaluate the effectiveness of a digital storytelling model in increasing information security awareness among smartphone users. The investigation was informed by the Protection motivation theory and unified theory of acceptance and use of technology. The study adopted a quantitative approach and used experimental research design in two phases of the study. The study population of the study included smartphone users in the cities of Nairobi and Eldoret. Simple random sampling was adopted to select a sample of 393 smartphone users in the first phase, and 277 smartphone users in the second phase. The main research instrument for the study was a questionnaire. The quantitative data was analyzed using descriptive statistical methods. The results showed that most Kenyan Smartphone users are aware of security threats facing them and are greatly concerned about related security risks. However, users still make poor behavioral choices related to the use of smartphones, making them vulnerable to cybersecurity attacks. One of the poorly adhered to security practices among participants was the use of public Wi-Fi. Consequently, this research uses a digital storytelling information security model to design a media that seeks to increase awareness on the use of public Wi-Fi among Kenyan smartphone users. The prototype was tested among 277 Kenyan smartphone users. The results indicate that digital storytelling was highly effective among an average of 65% of the participants in increasing the understanding of risks and secure behavior related to the use of public Wi-Fi. Further, the outcome indicates that an average of 70% of the participants had a high likelihood of adapting behavior that increases their security when using public Wi-Fi. Thus, the study concluded that digital storytelling is an effective method for increasing information security awareness among smartphone users. Based on these findings, the study recommended that a digital storytelling model approach can be adopted by smartphone manufactures, telecommunication companies, and information security organizations to promote behavior that will safeguard the privacy and security of end-users who utilize communication devices. In addition, the study recommended that information service providers and security agencies should include user needs and feedback when designing security awareness media; smartphone users should always practice secure behavior; and mobile applications should be regulated, and apps be ranked based on user security. In addition, software developers should develop more applications where by default the user data is protected.

TABLE OF CONTENTS

Declaration.....	i
Copyright	ii
Dedication.....	iii
Acknowledgement	iv
ABSTRACT.....	v
Table of contents.....	vi
List of Tables	viii
List of Figures.....	ix
Abbreviations and Acronyms	x
CHAPTER ONE: INTRODUCTION.....	1
1.1 Background of the study.....	1
1.2 Problem Statement.....	3
1.3 Objectives	4
1.4 Research questions.....	4
1.5 Significance of Study.....	4
1.6 Limitation of the Study.....	5
1.7 Delimitation of the Study.....	5
1.8 Assumptions of the Study.....	5
1.9 Operational Definition of Terms	6
1.10 Thesis Outline.....	7
CHAPTER TWO: LITERATURE REVIEW.....	9
2.1 Mobile Devices.....	9
2.2 Information Security	11
2.3 Mobile Security Issues.....	15
2.4 Information Security Awareness	18
2.5 Challenges Arising from Lack of Information Security Awareness.....	20
2.6 Digital Storytelling	21
2.7 Theoretical Frameworks	22
2.8 Summary of Opportunities and Gaps from Related Work.....	27
CHAPTER THREE: METHODOLOGY	28
3.1 Location of Study	28
3.2 Research Design	28
3.3 Target Population.....	31
3.4 Sampling Procedure.....	31
3.5 Instrumentation	32

3.6	Methods of Data Collection.....	34
3.7	Digital Storytelling Framework & Evaluation.....	36
3.8	Operations Definition of Variables.....	40
3.9	Data Analysis.....	41
3.10	Ethical Considerations.....	41
3.11	Application of PMT and UTAUT to the Methodology.....	42
CHAPTER FOUR: RESULTS AND DISCUSSION.....		43
4.1	Demographics.....	43
4.2	What is the information-security related behavior among Kenyan smartphone users?.....	46
4.3	What Digital Storytelling Model can be designed to address information security awareness among Kenyan smartphone users?.....	60
4.4	What is the Effectiveness of Digital Storytelling in Increasing Information Security Awareness among Kenyan Smartphone Users?.....	69
CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS.....		77
5.1	Summary.....	77
5.2	Conclusion.....	78
5.3	Recommendations for Further Research.....	79
5.4	Recommendations on Research Findings.....	80
5.5	Published Papers and Conferences from this Thesis.....	81
REFERENCES.....		82
APPENDIX 1: RESEARCH PERMITS.....		89
APPENDIX 1A: NACOSTI LICENSE.....		89
APPENDIX 1B: KeMU Introduction Letter.....		90
APPENDIX 2: QUESTIONNAIRE.....		91
APPENDIX 2A: PHASE 1.....		91
APPENDIX 2B: PHASE 2.....		96

LIST OF TABLES

Table 2.1 Summary of gaps and opportunities	27
Table 3.1 Shows the variables in the study	30
Table 3.2 Characteristics and process framework for designing the digital storytelling model	36
Table 3.3 Research design	39
Table 4.1 Smartphone user demographics.....	43
Table 4.2 Digital Storytelling Model user demographics.....	44
Table 4.3 Adaption of Figure 4.14 to an Information Security Belief Model.....	64
Table 4.4 Storyboard Illustration for an Information Security Digital Storytelling Model	65

LIST OF FIGURES

Figure 2.1: Smartphone adoption in Africa	10
Figure 2.2: Social engineering attack process (Mataracioglu & Ozkan, 2011).....	17
Figure 2.3:UTAUT (Venkatesh et al., 2003).....	25
Figure 4.1: Security features utilized by smartphones users	46
Figure 4.2: An illustration of Antivirus use.....	47
Figure 4.3: An illustration of Antivirus Installation on Various Gadgets	48
Figure 4.4: Awareness level of Security Risks	49
Figure 4.5: User perceived information security risk	51
Figure 4.6: Awareness on risk impacting security decision	51
Figure 4.7: Level of exposure influencing decision	52
Figure 4.8: Source of mobile applications	53
Figure 4.9: Factors considered while installing an application	54
Figure 4.10: Mindfulness of security messages during installation	55
Figure 4.11: Attentiveness to advertisement messages	56
Figure 4.12: Link verification before opening.....	57
Figure 4.13: Keeping pins and passwords confidential	58
Figure 4.14: Hierarchy of Contributing Factors towards Secure Behavior	63
Figure 4.15: Script	67
Figure 4.16: Screenplay	67
Figure 4.17: Previous Experience in Watching an Awareness Video or Advertisement	69
Figure 4.18: Video Evaluation.....	71
Figure 4.19: User understanding of security Concepts.....	72
Figure 4.20: Likelihood of embracing secure practices	74

ABBREVIATIONS AND ACRONYMS

DSM – Digital Storytelling Model

DS – Digital Storytelling

UTAUT – Unified theory of acceptance and use of technology

PMT - Protection motivation theory

IT - Information Technology

IS – Information Security

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

The mobile penetration rate in Kenya is 97.8% (Communications Authority of Kenya [CAK], 2018), partly as a result of the rise of a youthful population in the country, which has seen the demand for smartphones going up and the price of smartphones dropping (Jumia, 2019). The number of mobile users increased from 13 to 48.82 million users during the period of 2000 and 2017 (Statista, 2017). Besides, 99 percent of Internet traffic is through the mobile phones and other mobile devices (CAK, 2018). This explains why Kenyan mobile traffic was ranked number one globally (Statista, 2017).

The increased use of mobile phones has made Kenya a mobile-first economy (CAK, 2018). The mobile services have moved from traditional cash-in and cash-out economy to a key driver in financial inclusion and facilitators in Kenya Digital economy through the rise and evolution of services such as mobile loans, mobile savings, cross-border remittances and pay bills. Generally, seventy-five percent of the mobile transactions in Kenya happen through the mobile phone (CAK, 2018).

The huge rise in the rate of smartphone use in Kenya comes along with challenges of security. For example, mobile malware analysis reveals that 0.17% of mobile devices in the cellular network are affected by security threats (Raghuramu et al., 2015). While this percentage seems small, it is higher than the 0.0009% infection rate recorded in 2013. In addition, six million mobile application were analyzed and found that 15% contained malicious contents, although 37% were considered grayware (Paul et al., 2016). Certainly, this is a serious threat factor and hence useful to study because the amount of personal data, sensitive documents,

credentials stored that is processed by smartphones makes them an appealing target for attackers. Evidently, the increased interaction with smartphones poses a threat to users' privacy and security. For instance, cybercrime listed as an emerging threat (Kiboi, 2015), and an increased rate of cybercrime and cyberattack cases reported to the police (Serianu, 2018). Further, the cost of Cybercrime through mobile phones in 2017 was reported at 25 Million Kenya Shillings (Serianu, 2017b).

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). Also, a study carried out among 281 learners in Slovenia, investigating threat perception on mobile phones (Markelj & Bernik, 2015), showed that the learner population had little awareness of security threats and measures, thus education and awareness levels must be increased. These studies may imply that security awareness among Kenyan technology users is still low and hence they become easy targets for hackers. Therefore, for mobile phone users to better protect themselves, there is a need for increased awareness of potential risks that are associated with smartphone use. Consequently, user awareness could improve privacy and security among Kenyan smartphone users.

Digital Storytelling has been used to increase awareness for teaching children online privacy (Zhang-Kennedy et al., 2017), in information systems learning (Bromberg et al., 2013) and classroom training (B. Robin, 2008). The potential for this media in information security awareness includes construction of a security culture in organizations (Arsenijevic et al., 2016) and security trainings (Tschakert & Ngamsuriyaroj, 2019). Therefore, this research explores the use of digital storytelling to increase information security awareness among Kenyan Smartphone users. To be impactful such a model would first need an investigation of users'

level of security risk awareness in order to understand their behavior while using smartphones. Indeed, designing a model targeted towards information security users should be based on what users know and what they do (Kruger & Kearney, 2006). In fact, centering the users in the digital storytelling model is crucial since information security awareness has to be targeted, actionable, doable and provide feedback (Bada et al., 2015). This research aimed to address this need.

1.2 Problem Statement

Smartphones come with many security features, such as screen locks, pin, password, biometric, apps permissions, antivirus installation, whose use is solely determined by the decisions that users make and how they use them. Knowledge and sustained risk-free behavior on how to use such features to protect one's private information leads to decreased risks in cybersecurity attacks. However, there is limited information security awareness among Kenyan smartphone users, which in turn has led to issues such as increased cybercrime, theft of personal information, and financial losses. The increased rate of cyberattacks could mean that existing information security awareness models are not user-centered nor do they take advantage of digital media that could potentially impact behavior change. This research sought to design a digital storytelling model that takes into account current information security awareness and behavior among users. Thereafter, the research sought to create a digital media which was tested for effectiveness in increasing information security awareness among Kenyan smartphone users.

1.3 Objectives

Broad objective

To establish the level of security risk awareness and user behaviour among smartphone users in Kenya, in order to design a customized security awareness model with the aim of reducing information security risks.

To address the broad objective, this research sought to meet the following specific objectives.

Specific objectives

- i. To investigate information security-related behavior among Kenyan smartphone users.
- ii. To create a Digital Storytelling Model to address information security awareness among Kenyan smartphone users.
- iii. To measure the effectiveness of a digital storytelling model in increasing information security awareness among smartphone users.

To meet these objectives, this research sought to answer the following research questions.

1.4 Research questions

- i. What is the information security-related behavior among Kenyan smartphone users?
- ii. What Digital Storytelling Model can be designed to address information security awareness among Kenyan smartphone users?
- iii. What is the effectiveness of Digital Storytelling in increasing awareness of information security among Kenyan smartphone users?

1.5 Significance of Study

In addressing the research questions, this research is expected to make the following contributions; to identify various smartphone user behavioural gaps in security awareness and ways to curb them in an effective manner. Secondly, to provide insight on developing an

effective digital storytelling information security awareness model. Finally, to provide information to smartphone manufactures, telecommunication companies, information security organizations that can be used to promote behavior that will safeguard the privacy and security of end-users who utilize communication devices.

1.6 Limitation of the Study

This research mostly focused on smartphone users who live and work in urban areas. This limitation means that the needs and considerations for mobile phone users who live in rural regions might not have been considered. Also, the research did not study the effectiveness of other media (such as text) since only a digital storytelling media was implemented and tested. This limitation means that the impact of other types of media to increase information security awareness may not have been fully realized.

1.7 Delimitation of the Study

The smartphone proliferation in Kenya, including the rural areas, is at 97.8% (CAK, 2018). Data indicates that users in rural areas have a current ownership of 73% evidenced by increased access to use of social media sites like Facebook and WhatsApp (Kenya National Bureau of Statistics [KNBS], 2019). These statistics indicate that this research is generalizable to rural populations. In addition, while other forms of media, apart from digital video, were not used to create awareness, research indicates that the most preferred approach to address mobile security awareness among Kenyans is through media campaigns in the form of print, electronic, and social media (Okuku et al., 2015).

1.8 Assumptions of the Study

The researcher assumed that the sample size represented the picture of the entire population. Furthermore, the researcher presumed that one respondent represented response from one

person and neither as a representation of a group of people nor as an imposter of another participant.

1.9 Operational Definition of Terms

1.9.1 Behavioural Intention

Behavioral intention is an individual's plan to use a technology that directly affects their actual use (Iqbal et al., 2018), or the likelihood of a person having a repeated plan or decision (Leong & Karim, 2015). It is derived from the theory of planned action to define the likelihood that someone will engage in certain behavior (Wang & Liu, 2009).

1.9.2 Risk

Risk is defined within information security as the outcome of the possibility and the impact of a threat against the information assets of an entity (Giles & Marnix, 2010).

1.9.3 Threat

A new incident that has a potential to harm a system or a resource.

1.9.4 Vulnerability

Known weakness in a system or a resource.

1.9.5 User Awareness Definition

User Awareness can be defined as, knowledge compounded with attitudes and behaviors which serves to protect our information assets. The meaning of, being cyber security aware, is understanding what the threats are, and you are taking the right steps to prevent them (Jidiga & Sannulal, 2013).

1.9.6 Malware

Malware is any type of destructive software that can infect a computer or a mobile phone and interfere with its performance such as slowing down its processing speed, stealing personal information, and gaining access to unsecured areas of the device.

1.9.7 M-Pesa

M-Pesa is a mobile phone-based money transfer service, payments and micro-financing service.

1.9.8 Smartphone

Smartphone is a touchscreen mobile phone that has software functions which can download applications in its play store or internet.

1.10 Thesis Outline

Chapter 2: Literature Review

Chapter two gives an overview of the literature on user awareness, security frameworks and previous work that relates to digital storytelling for Information Security Awareness. In order to guide the structure of the chapter, discussion is divided into six parts: mobile use, security, mobile security issues, information security awareness, digital storytelling and frameworks. The chapter concludes with a summary of gaps and opportunities that have been identified in related work.

Chapter 3: Methodology

Chapter three outlines two phases of the methodology that were used to achieve the research objective. The framework that forms the basis of the digital model adopted is presented in this chapter as well as the research procedure seeking to understand user-related behaviour. The

chapter discusses a two-phase process describing how the research was conducted. Further, the chapter describes the participants who took part in the study, ethical clearance, the data collection methods, data analysis and digital storytelling framework. Thereafter, the research process followed to address the research questions is presented. The chapter concludes by describing a summary of the research procedure to address the research questions.

Chapter 4: Results and Discussion

In this chapter, the results and analyses of the collected quantitative and qualitative data as per the evaluation metrics used to address the research questions are presented and discussed. The chapter starts with a discussion of the participants who took part in the study and a review of how they participated in the experiments. Thereafter, this chapter reports the results from the two phases of the study. The chapter concludes with a summary of the research findings

Chapter 5: Summary, Conclusions and Recommendations

This chapter begins by summarizing the thesis research questions, and presents the conclusion based on the results. A synthesis follows of how the research findings addressed the research questions. Thereafter, the chapter discusses the recommendations from the study. Finally, the chapter discusses the suggestions for future research work.

CHAPTER TWO

LITERATURE REVIEW

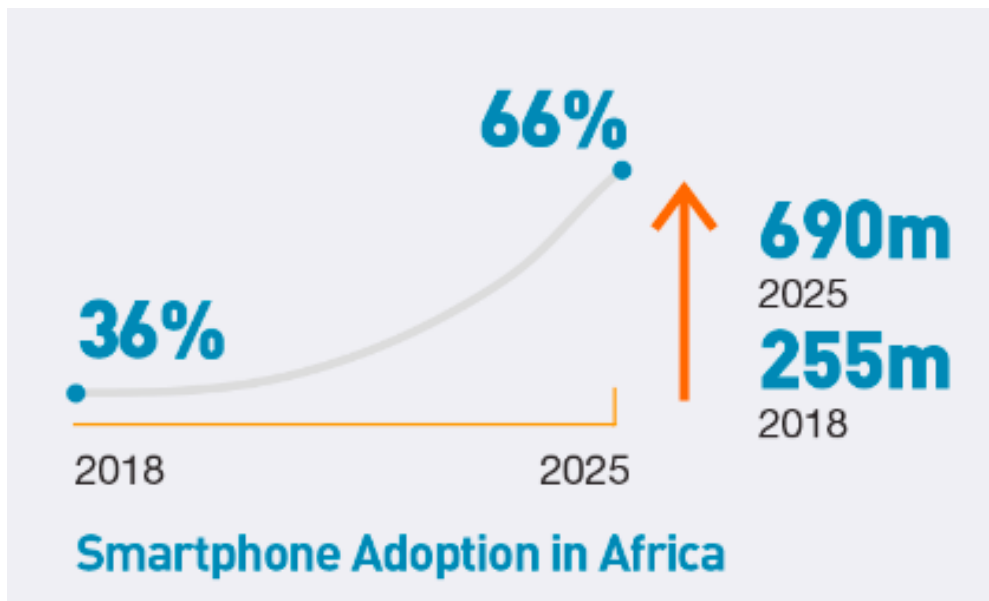
The aim of this research was to establish the level of security risk awareness and user behaviour among smartphone users in Kenya, in order to design a customized security awareness model with the objective of reducing information security risks. Therefore, this chapter begins by reviewing the use of mobile phones, followed by an analysis of information security risks and issues. Information security issues among smartphone users can be tackled by increasing awareness. Therefore, this chapter presents a review of related work that address information security awareness. Thereafter, the chapter reviews literature on digital storytelling as a potential approach to increasing awareness among Kenyan smartphone users. The frameworks underpinning this study are then presented. The chapter concludes with a summary of gaps and opportunities identified from the related work, which form the foundation of this study.

2.1 Mobile Devices

Mobile phone penetration in Africa is skyrocketing as more people are becoming connected and depend on mobile use for communication. In South Africa, for example, nine in ten adults own a mobile phone while Ghana has a rate of ownership at 80% and Senegal at 79%. Nigeria and Kenya are at 80% of ownership just like Ghana, followed closely by Tanzania at 75%. The most used mobile phone is a feature phone. Further, mobile applications in 2013 were 5,000 and increased to 30, 000 in 2017 (Jumia, 2019). The adoption of mobile phones and especially smartphones are projected to rise even more as more affordable phones are flocking the market. This rise is also attributed to the increase in a youthful population. **Figure 2.1** shows the projected adoption of mobile phones over the next five years.

Figure 2.1:

Smartphone adoption in Africa



The use of mobile phones is mainly among the educated population (Silver & Johnson, 2018). Consequently, mobile Internet use is rising and is especially beneficial in personal lives and also for economic reasons. Countries with higher mobile access have more successful economies. Without mobile access or broadband, rural nations lack enough resources in expanding its gross domestic product (GDP). Mobile phone use also makes significant contributions in schools to support classroom learning (Pew Research Center, 2015). There are also institutions that have fully adopted online learning especially institutions of higher learning like universities and colleges. Students are specifically considering mobile devices due to their portability and they can utilize internet using public WiFi connections which, are readily available inside and outside of their institutions. Mobile data is also becoming more affordable with availability of different range of data packages to choose from. There is a projection that by the year 2025, 690 million smartphones will be used in Africa (Jumia, 2019). These trends show that mobile phones are an everyday tool that is essential for communication, learning and playing.

Mobile phones have moved from the traditional use of calling and short text to instant messaging, emailing and social media use. Mobile use in Kenya has transformed the financial sector by being a driving force in the digital economy, because of the adoption of services such as mobile savings, mobile loan, pay bills and money transfer across borders. Certainly, 1.4 trillion Kenyan shillings were transacted within three months between the month of April and June 2018 (CAK, 2018).

Smartphones contains many free and paid built-in applications such as camera, email, web browsers, which are available in their respective online stores. These mobile-based applications like WhatsApp have also facilitated communication, as it is an easier way to send multimedia apart from offering cheaper calls option especially across countries. For example, it has been used to facilitate communication among student health volunteers (Farmer et al., 2016). Mobile usage is going to increase in use now that the infectious virus Covid 19(Corona Virus) has changed the way learning is done. More smartphone users are installing several applications on the phone for online meetings, classes and exams. A smartphone is becoming a necessity as users become dependent on using the Internet. Because of the increase in demand, mobile phone manufacturers are also improving the smartphones they are producing to be available at affordable prices. Due to the increase in use of mobile phones, the amount of information on the mobile is going to increase significantly, ranging from private use to institution and organization use. Therefore, it is necessary for Kenyan users to be able to safeguard such information by adopting better security practices.

2.2 Information Security

SANS institute indicates that Information Security are the processes and methodologies that are meant to protect information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. Information can range from an email, employee's information, medical records and even personal profiling. The information stored on mobile

phone is private and should not be disclosed without the consent of the owner because the risk of losing such information is devastating. The information loss can happen in different ways including financial and personal data (Honan, 2016). The loss can affect intellectual property while other losses can be life-threatening (Syssec, 2013). Information loss can lead to denial of services to avoid calling emergency numbers, access mobile money apps, malicious location-based services, leakage of GPS coordinates and control of devices connected to a mobile phone such as cars. The result can be user profiling, account compromise or identity theft.

Lack of user awareness on risks can cause huge financial losses (Androulidakis, 2016) because users are either unaware or uninterested in the potential risks (Ophoff & Robinson, 2014). Consequently, there is a security advantage for those users who are risk-aware (Gkioulos et al., 2017), hence there is a great need for users to understand information security. Furthermore, legislation should be effective to protect users. Some countries have adopted policies to protect their citizens. Example of these policies include: GDPR (General Data Protection Regulation), which is a European Union Legislation, that aims at protecting personal data and allowing free sharing of such data. It details obtaining consent while collecting data, explaining why you need the data and if a different need arises while using the data, the subject has the right to know. The user also has a right to be forgotten or opt-out of a study.

There are countries like the US and UK who have adopted the new regulation and amend their Data Privacy laws accordingly. For instance, the Data Protection act 2018 of UK main purpose is to protect the people's rights and privacy and to ensure that the data about persons that is used by organizations is managed properly. On the other hand, although the Kenyan government has made strides on Data Protection law 2018, which is aimed at protecting personal data, the country is yet to adopt a specific data protection legislation. Data protection law will see more organizations and individuals taking personal responsibility in handling data.

Then again, securing of information should provide solutions that are easy to use and implement. Too much security without usability creates more problems. For information security to be effective, there is need to understand how risk is assessed;

Risk Assessment

Whereas threat likelihood is assessed based on experience and statistics, vulnerabilities, existing controls and how effectively they may reduce vulnerabilities, risk assessment is calculated based on a risk matrix (Standard, 2011). Risk can be mapped as Low (0-2), Medium (3-5), or High (6-8). Since each threat is associated with specific security attributes, the relevant asset impacts are taken into account (Theoharidou et al., 2012). Top Ten Smartphone Security Risks, that was used to structure questionnaires in this study, according to the European Union (Giles & Marnix, 2010) are as follows:

High Risk;

R1 Data leakage occurs when a stolen or lost phone with unprotected data allows an attacker to access it.

R2 A risk that happens when the phone is transferred to person without removing sensitive data, allowing an attacker to access its data.

R3 Unintentional data disclosure, which occurs when most apps have privacy settings but users are not aware that the data is being transmitted.

Medium Risk;

R4 Phishing happens when an attacker collects user credentials (e.g. passwords, credit card numbers) using fake apps or (SMS, email) messages that seem genuine.

R5 Spyware that happen when a phone has a software installed allowing an attacker to access personal data. Such malicious software includes software requesting and abusing excessive privilege requests.

R6 Network spoofing attacks occur when an attacker deploys a rogue network access point and users connect to it. The attacker then intercepts the user communication.

R7 Surveillance which refers to spying on someone with their targeted smartphone.

R8 Diallerware where an attacker steals money from someone using malware that hides the use of premium numbers.

R9 Financial malware, which is designed for stealing financial information such as credit card numbers.

Low Risk;

R10 Network congestion is when the network resource becomes overloaded due to smartphone use leading to network unavailability for the subscribers and users.

Some of the security measures that smartphone users can use to protect themselves include:

i) Physical control, which ensures that data isn't readily available in case the mobile is lost.

The measures include the use of a pin, biometrics or password. If a device is being transferred to another user, all the data should be erased.

ii) Network connection which consists of two main types of attack for mobile phones. The first is when a phone connects to the Internet. The second is when a phone connects to an existing network.

iii) Mobile devices are designed to ease finding, acquiring, installation, and use third-party applications from mobile application stores. Applications platforms exposes the mobile security risks, from application stores and platforms that do not have sufficient security restriction or other measures on third-party application publishing. Further, even if the application store is well secured, there will be an existing risk if someone installs suspicious applications.

iv) Untrusted contents like QR codes can easily expose user data. Untrusted content doesn't vet the URLs its connecting to.

v) Sometime keeping the locational services on can expose the user, as it can be mapped to his activities.

vi) Phone Updates- Most updates released are fixes to a flaw. Users need always to keep their applications and Phones updated.

The above are examples of measures to protect smartphone use. Although, most users are not aware of all these. Consequently, smartphone users best practices such as the installation of applications from known sources only (Dimensional Research, 2017), detection and blocking of fraudsters messages (Ali, 2017), detection and blocking of fraudsters call (Cukier et al., 2012), keeping pins and passwords confidential (Thomas et al., 2015), are encouraged.

2.3 Mobile Security Issues

Smartphones access, store and retrieve a lot of personal information. Some of which are solely stored on the phone like Photos, Texts, Calls, Mobile banking Apps and application messages such as WhatsApp. Therefore, the information should remain private. Hence the need for mobile security. Risk can happen in mobile phones through many forms such as loss or deletion of data, confidential leakage of information and loss of money through leakage of mobile money pin such as M-Pesa. Most of these risks that cause security breaches are caused by malwares, hackers and fraudsters.

Malware

Research reports that about 90 percent of Android devices are exposed to at least one major threat (Thomas et al., 2015). The vulnerability model happens in three ways. First, through the installation of an application that has malicious code. Secondly, through already installed app installing malicious code. Thirdly, an attacker puts the malicious code directly into the system (Thomas et al., 2015). Such risks call for all smartphone users to be more careful when using their smartphones, so that their data can be secured.

16.27 percent of Kenyans using smartphones have been affected by malware (Statista, 2019). However, malware can be detected and protected (Arshad et al., 2016). In addition, a literature review can be used for a personalized case study, in order to protect yourself from malware (Ali, 2017).

Hackers

In Kenya, hackers mainly target banks and mobile money vulnerabilities because the probability of being paid ransomware is high. Hackers usually look for any vulnerability in a system and exploit it. Non-secure username and password gives the hacker a chance to succeed, and this applies to smartphone too. Typically, every 39 seconds, an hacker attacks (Cukier et al., 2012).

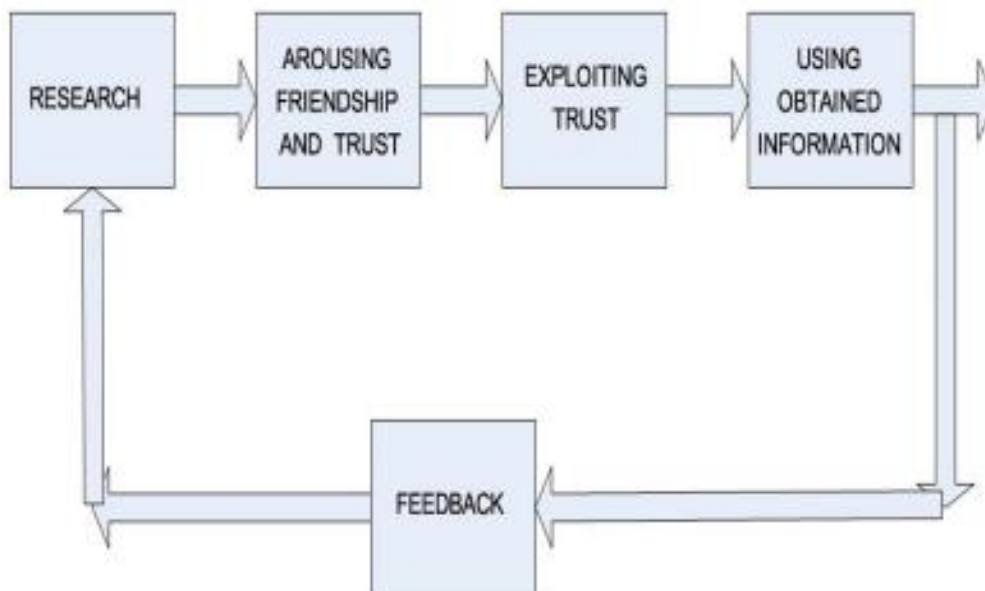
Hackers takes advantage of Social Engineering as it is attack directed to the user because a greater percentage of information security depends on the user, while technical measures influence vulnerabilities only to a small percentage. Security breaches often happens when a seemingly nice person gets information that looks trivial, and the user doesn't see any reason to protect it. Most social engineering attacks are sophisticated but reaches the user as simple and direct. Hackers do this by gaining trust, and they go ahead and prepare for any questions that a user might have. Social Engineering happened to Safaricom users in Kenya, where users were being called and asked for their sim-card pin. Those who shared the pin found out that their sim cards had been swapped (Stenitzer, 2015). Attackers also take advantage of peoples desires for free or lucrative deals. Hence users may fall victims by being expectants of good things. Some research had shown positive steps when social engineering attack were performed, however, some sensitive information can be easily found online or can be accessed easily through a cell call by a novice social engineer (Fincher & Hadnagy, 2015). Even though most social engineering is done at an organization set-up, the results reflect how successful social engineering can happen to a smartphone user. This was further shown in Kenya in the year 2007

and 2018, when some employees in a top mobile company were dismissed because of fraud charges (Safaricom PLC, 2017).

The social engineering attack process is shown in the **Figure 2.2** below (Mataracioglu & Ozkan, 2011). The first stage is the research process. At this stage, the attacker obtains a lot of information about the user. The second stage is forming friendship and trust where the attacker tries to get victims sympathy. The third stage is when trust and friendship is exploited to obtain user information.

Figure 2.2:

Social engineering attack process



Note. (Mataracioglu & Ozkan, 2011)

The information found is then evaluated. If the information is sufficient, the attack is successful. If the information is insufficient, the social engineer goes back to the initial stage, to try and repeat the process.

Fraudsters

Fraud may happen in several ways on mobile. Through free apps, a fraudster can include subscription to a premium SMS service. Fraud can cause financial losses and the possibility of being given bad credit score on credit reference bureaus, hence damaging someone's

reputations. Fraud also happens through impersonation as a cell call center or major lottery that is happening. The smartphone users are lured into believing that an authority is calling them hence sharing private information or money in the hope of getting service. Information leakage can adversely affect the user by the fraudster taking over the accounts forever like the case of sim swap or email control.

In conclusion, users need to be aware of malware, hackers and fraudsters. That is why user awareness is important because the consequences of information loss can be catastrophic.

2.4 Information Security Awareness

Information security awareness is not just knowledge, but it is also knowledge that results into action such that security awareness is combined with sustained behaviors that serve to protect one's information. Being information security aware means that someone understand what the threats are and they take the right prevention mechanisms (Martin, 2014). Information security awareness is also the extent to which users understand the significance of information security, the level of security required by an organization and their individual responsibilities (Chaplin & Creasey, 2011). Such security awareness requirements can also be applied to smartphone users.

Considering the measurement of user security awareness, researchers have attempted to establish precisely what to measure, such as a model to measure the information security awareness of an individual focused on three metrics: knowledge (what users know), attitude (what users think or feel), and behaviour (what users do) (Kruger & Kearney, 2006). Knowledge-based institutions also suggest that raising the state of awareness, through policies, leads to improved behaviors and attitudes regarding information security (Ahlan et al., 2015); knowledge awareness through policies is also acknowledged at an individual level (Mathisen, 2004). They present a number of ways to measure security awareness levels, including periodical surveys to employees of an organization, personal interviews and group forums.

Unfortunately, gauging such awareness is not a trivial task. When someone participates in a security awareness program, its effectiveness can be checked by determining the individual's knowledge before and after the intervention. Nevertheless, the user know how does not imply that they demonstrate such every other time. There is a need for constant reminders so that users cannot go back to their previous levels of awareness. Effective security awareness is affected by shared attitudes, norms, values, individual perceptions, work behaviors and practices that characterize a group or organization (ENISA, 2010).

Previous research has been done on how security and privacy-related decisions by smartphone users are affected by their attitudes, perceptions, and understanding of various security risks (Alsaleh et al., 2017). Also, there is security complacency among users while downloading unverified apps from play store and third parties (Mylonas et al., 2013). Further, smartphone users who download apps tend to be unaware of security risks associated with downloading from online repositories (Mylonas et al., 2013). Users believed that the controlled app market, for example Google Play, is secure (Mylonas et al., 2013).

To understand if people are wary 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 (Paul et al., 2016). Risk behaviour 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 that sought to investigate the security adoption and awareness 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 et al., 2015). These results demonstrate that awareness of information security varies depending on the subjects and their 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) as Three-quarter of the Kenyan population is under the age of 30 hence they are deemed comfortable utilizing most of the features in a smartphone (KNBS, 2019). Therefore, there is a need to understand the behavior of smartphone users while using mobile phones. This thesis addresses this need, specifically for mobile phone users in Kenya who are adopting technology really fast in comparison to other Africa countries (Serianu, 2017a).

2.5 Challenges Arising from Lack of Information Security Awareness

Kenya has been affected by various cyber-attacks, which have adversely affected the population, making cybersecurity experts to warn that cybercrime in Africa is at a high level and can cause devastating effects, yet less is being done to counter it (Oladipo, 2015). Kenya currently stands at number 42 in the list of the most attacked countries in the world (Kaspersky, 2020a). Specifically, the main malware types that attacks are: Cryptominer, Botnet, and Mobile (Check Point Software Technologies LTD., 2020). The attacks are mainly affecting the internet users, government officials, and worse, the financial sector. However, a lot of focus has been mainly on buying hardware and tools. These tools are good, but there is need to understand the technologies behind this plus the users using these technologies.

The need to understand the technologies is also because of the changes in the nature of cyber-attacks as a result of emerging technologies. The human element is weakest link for attack hence there is need for cybersecurity awareness in Kenya. Coincidentally, previous reports on cybersecurity in Kenya was focused on tools that could be used to prevent cybercriminals.

Recently, the reports have focused on situation awareness. Companies and people are urged to understand technologies behind their ICT infrastructure, and people they are working with including their customers. Undoubtedly, the reports are now addressing what other people or organizations are practicing locally instead on focusing on the worlds outlook like before (Serianu, 2017a). The challenges faced by a lack of information security awareness among smartphone can potentially be addressed by the use of digital storytelling towards impacting behavioral change.

2.6 Digital Storytelling

One approach that has been used to increase the awareness of information security is through experience sharing. For example, users reported that they would change their behaviour based on the security stories they had heard; especially if the stories had a serious lesson or if it was from knowledgeable sources (Rader et al., 2012). A form of experience sharing utilizes digital media in the form of digital storytelling, which is the combination of various forms of multimedia like images, audio, and video to tell stories (B. Robin, 2011).

Digital storytelling has been used to develop awareness on online cyber risk such as Internet addiction, pornography, game addiction and bullying, among 10 to 14-year-old's (Khalid & El-Maliki, 2020). Further, it has also been used in an organization to form an effective information security culture, motivating employees, build a positive image and control crisis (Arsenijevic et al., 2016). Indeed, the advantage of storytelling is that apart from its instant behavioural change, it has the highest retention rate (Skinner et al., 2018). There are three types of digital stories (i) historical documentaries that describe past events; (ii) personal narratives in which the authors express personal experiences; and (iii) stories that inform or instruct the viewer of a particular content (B. Robin, 2008). This thesis designs a digital storytelling model that informs smartphone users on information security practices.

Seven elements have been cited as contained in digital storytelling (Center for Digital Storytelling, 2005); (i) a point of view or perception that describes the view of the creator; (ii) an important question to be answered by the end of the story; (iii) an emotional approach that addresses various issues while relating to personal experiences; iv) the author's voice that contextualizes the story; v) a powerful soundtrack from sounds that support the narrative; vi) economy that refers to utilizing a short enough narration to tell the story without overburdening the viewer's attention; and vii) using a pace that users can follow so that the story neither progresses too slowly or too quickly. This thesis implements all these seven aspects while underpinned by theoretical frameworks that support the understanding of users before designing new models and technologies to serve them.

2.7 Theoretical Frameworks

This section reviews the theories related to the study. A theory is a description of interrelationships that shows how and why something occurs (Corley & Gioia, 2011), and consists of assumptions, principles, and procedures to extrapolate the behaviour of a specified set of events (Weick, 1995). Protection motivation theory (PMT) and Unified theory of acceptance and use of technology (UTAUT) has been a great insight in building up the literature of this study

2.7.1 Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) aims at describing how people are motivated to behave in a self-protective way towards a perceived threat or risk (Rogers, 1975). PMT theory predicts how people cope and make decisions to protect themselves after receiving fear-arousing recommendations. It suggests that when faced with a threat, individuals react in two assessment process, one is focused on the threat itself and another is knowledge to act against the threat. It is mainly used to explain the decision behind threats.

When focused on the threat itself, people tend to consider how negative the threat is and the possibility of the threat coming to pass such that it can directly affect them. The negative result of the threat can lead to avoidance or denial (Weber et al., 2002). While in, people will assess if undertaking the recommended response will eliminate the Threat considering their level of confidence in carrying out the acting (Conner, 1996). It may lead to adaptive behaviors as the cost of response is very high. How users react to Threat may deduce that people behaviors are influenced by what they believe and know and not by the real reality. PMT seems to be well suited to the behavioural context of security awareness because the primary goal of securing mobile phone is triggered by risks which is a fear-arousing stimulus.

Critique of Protection Motivation Theory

It does not take into consideration variables like perceived barriers, which can be used to help in understanding the cognitive process in PMT. Besides, it does not account for situations which they have never been trained to deal with.

Contributions of Protection Motivation Theory

The theory has been widely used in cybersecurity in, designing prompts to influence online behavior's (van Bavel et al., 2019), improving online password security and invasion ways (Jenkins et al., 2014), to increase awareness on safety procedures during natural hazards (Westcott et al., 2017), online virus protection behaviour (D. Lee et al., 2008), persuading

Internet users to protect themselves(Jiang et al., 2016), 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 et al., 2008).

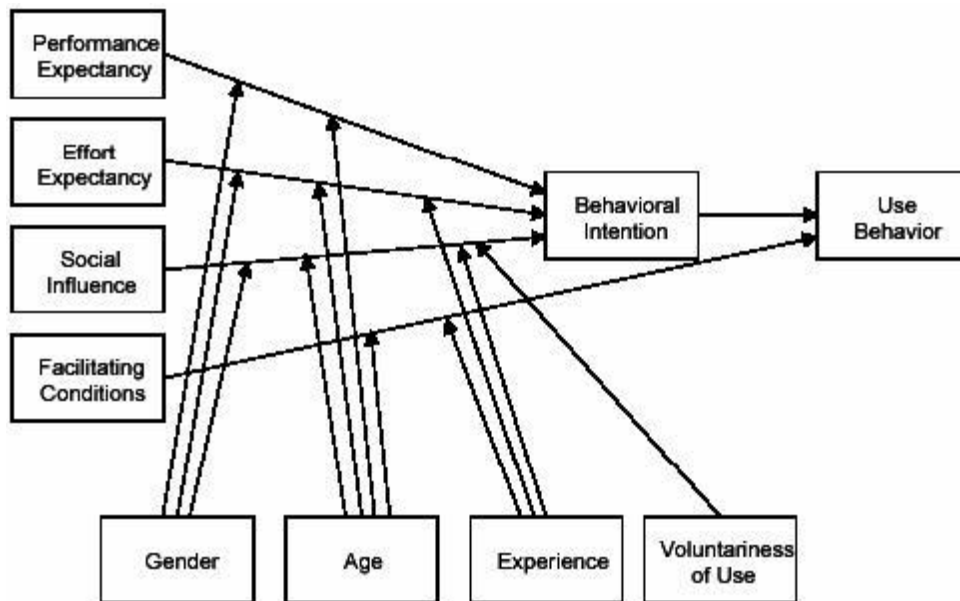
In this study, PMT assisted in understanding behaviour of smartphone users especially in relation to risk, as information security is a form of risk.

2.7.2 The Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT seeks to demonstrate the intention of users to use information systems and later used to explain usage behaviour (Venkatesh et al., 2003). It synthesized the models in the theory of Planned behaviour together with the Technology acceptance theory to develop the Unified theory of acceptance and use of technology (UTAUT). 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 behavioural intention to use a technology and actual technology used primarily in organizational contexts. Below is a diagrammatic representation showing relationships between user behavior about facilitating conditions and behaviour intention. It also represents the relationship between performance expectancy, effort expectancy, social influence to behavioural intention.

Figure 2.3:

UTAUT



Note. (Venkatesh et al., 2003)

(Venkatesh et al., 2012) proposed and tested UTAUT2, which incorporates new constructs, hedonic motivation, price value, and habit which focus on new theoretical mechanisms (Venkatesh et al., 2016). The theory has been used for use and acceptance of consumer context (Venkatesh et al., 2012), online purchase of tickets of low cost carriers (Escobar-Rodríguez & Carvajal-Trujillo, 2014) and students acceptance for eLearning in Saudi Arabia (Nassuora, 2013)

Weakness of UTAUT

UTAUT lacks the aspect of trust as one of the constructs in theory (Venkatesh et al., 2012). In addition, UTAUT omits an important aspect of attitude of individuals towards the technology yet adoption is strongly influenced by anticipated benefits (Venkatesh et al., 2016)

Contributions of UTAUT

The contributions that the UTUAT model makes are: Firstly, refining contextual system habits to feature-level use. Secondly, adding a new library of contextual effects with a new focus on job performance outcome, and finally, it incorporates time and events in the contextual moderation (Venkatesh et al., 2016).

UTAUT also borrows the following contributions from other models; Firstly, the model describes a substantial proportion of varying use of intentions and behaviors among a number of information technologies. Secondly, it is a robust, powerful, and cheaper framework for predicting if and how users will accept a technology. Lastly, UTUAT has been used in many studies and has proven to be of sound quality and statistically reliable.

In this research UTAUT assisted in understanding how users are using their smartphones and the behaviors they exhibited. It helped in solving the first objective of this research. It also helped in research two as it gave guidance on what to include in model creation that could bring impact.

2.8 Summary of Opportunities and Gaps from Related Work

The gaps and opportunities identified from the related work, which motivated this study, are summarized in Table 2.1 below.

Table 2.1

Summary of gaps and opportunities

Opportunities	Gaps
Increased use and penetration of mobile devices, including smartphones.	Increased cases of mobile security vulnerabilities such as financial threats, social engineering attacks, and malware invasion.
The advantage of storytelling is that apart from its instant behavioural change, it has the highest retention rate. Hence, existing frameworks on digital storytelling that can be explored.	Limited user-centered information security awareness models, which are underexplored in Kenya.
Protection Motivation Theory (PMT) helps in understanding behaviour on how individuals are motivated to react in a self-protective way towards a perceived threat.	Limited evaluation of the impact of information security awareness media on the
UTAUT models explains user intentions while using information systems and also used to explain usage behaviour.	potential of behavior change.

CHAPTER THREE

METHODOLOGY

The purpose of this research was to investigate the effectiveness of digital storytelling in increasing information security awareness among smartphone users and potentially influence their security-related behaviour. Thus, the first step was to understand the level of user awareness. To achieve this, an online questionnaire was used to understand user knowledge and the security measures utilized. The feedback informed the design of a digital storytelling model. To undertake this research process, the target population is first described in this chapter. Thereafter, the data collection tools and analysis methods are presented. To meet the objectives of the study, a digital storytelling framework is discussed, which would be used to design the digital media. The chapter concludes with a summary of the research process that was followed to address the research questions of this study.

3.1 Location of Study

This study was conducted in Nairobi, Capital City and a small city, Eldoret in Uasin Gishu County to increase the accuracy of data by reducing bias on awareness due to their level of exposure based on geographical location. The total population of Nairobi and Eldoret is approximately three million residence. The mobile penetration rate of Kenyans is 97.8% (CAK, 2018), the research considered the total population of Nairobi and Eldoret cities, estimated at 6 million people.

3.2 Research Design

A research design is defined as the blueprint or detailed plan that is followed to complete the study. It ensures that the study is relevant to the problem and uses economic procedures (Kothari, 2004). It is summarized as a set of methods or procedures that are chosen by a researcher. It describes how, when, and where data will be collected and analyzed concerning the research objectives. The procedural plan that is endorsed by the researcher should be valid, objective, economical and accurate when

answering questions (Kumar, 2011). There are various types of research design including case studies, cohorts, cross-sectional, descriptive, experimental, exploratory, correlational and observational (Kumar, 2011).

The research design is presented to show how the following three research questions were addressed using the already discussed methodologies.

RQ1: What is the information security-related behavior among Kenyan smartphone users?

RQ2: What Digital Storytelling Model can be designed to address information security awareness among Kenyan smartphone users?

RQ3: What is the effectiveness of Digital Storytelling in increasing awareness of information security among Kenyan smartphone users?

In order to answer these three research questions, a two-phase research process was followed as shown in Table 3.1 below.

The Pilot Phase addressed the first research question which investigated information-security related behavior among Kenyan smartphone users. In this phase 393 Kenyan smartphone users' results were analyzed on how they are aware of various risks in their phones, their concern for smartphone threats and what measures they were using to protect themselves.

The Implementation and Evaluation Phase, which was as a result of Phase 1, addressed the second and third research questions. The second research question was aimed at designing a Digital Storytelling Model to address information security awareness among Kenyan smartphone users. The digital storytelling model was achieved by comparing different models, frameworks, and literature. The Digital storytelling model led to the design of a video that was shared among Kenyan smartphone user in order to test its effectiveness. The third research question then measured the effectiveness of the model

3.2.1 Experimental Design

This research implemented experimental design by defining independent and dependent variables based on research objectives. The digital storytelling model, which is the dependent variable, was affected by the changes in either security awareness, risk perception of smartphone users or security countermeasures. Questionnaires were created to test the three defined research questions among smartphone users. The questionnaires asked the right questions, in a clear, and efficient manner. Then, the generated data was analyzed.

Experimental design was chosen as it is best in reducing variability of the results in a study. Experimental design gives a better picture in understanding how independent variable affected dependent variables.

Table 3.1

Research design

Phase	Research Questions	Methodology
Phase 1-Pilot	RQ1	Exploratory Survey
		393 Participants
		PMT Framework
	RQ2	Formulating Digital Storytelling Model
Phase Implementation and Evaluation	2- and RQ3	Design of Digital Video for Experimental purposes
		Evaluation Survey
		277 Participants
		UTAUT Framework

in increasing awareness and potentially influencing the security-related behaviour among Kenyan smartphone users. The video created was shared alongside the evaluation questionnaire, which was completed by 277 smartphone users in Kenya.

3.3 Target Population

“Population” or “universe” are the items that a researcher is considering in the study (Kothari, 2004). This study population whether it is individual, group or communities, are the people whom information is collected from them (Kumar, 2011). A full description of all the items in the “population” is referred to as a census inquiry. If the study is done to the total population, then it is referred to as a census survey where the best accuracy is obtained.

This study was conducted among smartphone users in Nairobi, Capital City and a small city, Eldoret in Uasin Gishu County to increase the accuracy of data by reducing bias on awareness due to their level of exposure based on geographical location. The total population of Nairobi and Eldoret is approximately three million residence. The mobile penetration rate of Kenyans is 97.8% (CAK, 2018), hence to calculate the sample size, the research considered the total population of Nairobi and Eldoret cities, estimated at 6 million people.

3.4 Sampling Procedure

A good sample population lies within 10 to 30 percent of the entire population (Mugenda, 1999). In this study, the target population which is Nairobi and Eldoret have a population of 5,560,259, which represent 12 percent of the Kenyan population (47,564,296) (KNBS, 2019). Furthermore, a sample is the number chosen from the population to constitute a sample and are effective, representative of the population, reliable and flexible (Kothari, 2004). Thus, the sample size should not be too limited or too large, but should be the right size (Kothari, 2004).

Assuming a population proportion of 0.5, 6 million population size of Nairobi Residence including Eldoret in Uasin Gishu County, and a confidence interval of 95% where z or 95% confidence level is 1.96.

To calculate the sample size, the research used the formula below;

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

where

z is the z score

ϵ is the margin of error

N is population size

\hat{p} is the population proportion

This study was conducted in two phases, a pilot phase and an evaluation phase. The 384 participants were targeted for the pilot phase. The sampling calculation was also used in the evaluation phase, considering a confidence interval of 95%. Where z or 95% confidence level is 1.96, 420 population size and population proportion of 0.5. Thus, using the same formula in phase 1, the sample size was expected to be at least 201 random smartphone users, to reduce bias. The sampling targeted a fair representation of each gender. There was also an intent to sample a mix of people from different educational background and age. Study participants were randomly selected Kenyans. Random sampling was appropriate because it gives a fair chance for each sample to be chosen and sampling error can be estimated. Moreover, the samples are unevenly distributed throughout Nairobi and Uasin Gishu County, Kenya.

Participants were recruited through an email invitation, social media platforms and fliers. Participation in the research was open to users of any mobile operating system.

3.5 Instrumentation

Validity and Reliability

The validation process seeks to highlight issues or biases in the methodology, and any potential effect of these on the study (Rojon & Saunders, 2012).

There are advantages of the online survey, which are:

- i) It can reach so many people, hence suitable for a large audience.
- ii) Flexibility in survey can be delivered.
- iii) Respondents get the convenience of answering the questions anywhere anytime.
- iv) Data entry and analysis can be done online using google sheets.
- v) There is absence of interviewer bias hence anonymity of the respondent (Wetzel, 2010).

On the other hand, shortcomings of online survey exist, such as:

i) Potential ambiguous questions can be the most significant drawback (Rojon & Saunders, 2012), as the researcher may not necessarily be present to clarify any unclear questions. This limited contact with the researcher can limit the opportunity for participants to further probe for in-depth details the way an open-ended interview or focus group could allow.

ii) The response rate might be low, and can then undermine the anticipated validity and credibility of the collected data (Saunders & Rojon, 2014).

In this study, to minimize these risks, a test survey was sent to 20 individuals in the pilot phase and 10 individuals in the evaluation phase, to seek feedback on errors so that there is assurance that the respondents would not have any challenges while answering the questions (Rojon & Saunders, 2012). Moreover, on the random design that the research used, although random sampling can be a clear representation of the entire population, some other respondents can refuse to answer the survey (Kumar, 2011). The research mitigated this by getting to know why the respondents declined to answer (Saunders & Rojon, 2014).

3.6 Methods of Data Collection

The research study was based on quantitative and qualitative research methods using a sample of a large population. The quantitative research method is used to show relationships of variables so as to explain, predict and control scenarios (Kothari, 2004). The qualitative research method intends to understand the opinions, behaviors and attitudes of the sample population. It answers the questions of what, how or why of a phenomenon (Kothari, 2004).

The study used an online survey through google forms online questionnaire. Online survey allows questions preview before sharing, collecting of data provides a friendly interface, and can be used to reach many respondents irrespective of their geographical location. Consequently, enabling us to get in-depth social and behavioral understanding. Offline questionnaires were also utilized where the questions were printed for any user who had no access to the Internet. Some of the questions were closed-ended while some were open-ended. A mixed type of questions was used because the study needed to understand user behaviour without influencing the participant.

Questionnaire Structure

The study was conducted in two phases - pilot and evaluation. For the pilot, the questionnaire that was used to collect data is attached in Appendix 2A.

In the pilot phase study, to minimize any potentially ambiguous questions and to validate the survey, the questionnaire was sent to 20 individuals before the study commenced. Testing process was important to seek feedback and ensure that respondents would not encounter difficulties when answering the questions. The survey contained 42 questions. The questions were divided into parts, each focusing on a specific area:

- i) The section on Demographics sought to determine the background of the participants in terms of age group, gender, IT knowledge, setting they lived in, type of phone, and their profession.

ii) The section on Smartphone Use was designed to understand the type of smartphones the participants owned, what they used it for and what data they stored on it. This section of the survey also sought to understand where the participants downloaded applications from, what factors they considered when installing an application and whether they believed that the applications they downloaded had any prior security review.

iii) The section on Security Threat Awareness sought to understand of the participant's general security awareness associated with smartphone use.

iv) The section on Perceived information security risks outlined several issues that could compromise the security of smartphone users. Smartphone users were asked if they were aware that the particular security issue would happen and if they are concerned about it occurring to them.

v) The section on Mobile information security countermeasure awareness sought to determine what security mechanisms the users used to protect themselves from security threats.

In the evaluation phase collection, the questionnaire that was used to collect the data is attached in Appendix 2B. In this phase, to minimize any potentially ambiguous questions, a testing questionnaire was sent to 10 individuals so that they could give feedback on the quality of the survey and ensure that respondents would not have problems in answering the questions. The survey contained 11 questions. The questions were divided into sections, which was focused on a specific area:

i) Background Information-The questions was meant to know where the participants resided and some demographics of the respondents was aligned with the pilot phase.

ii) Video Evaluation- The questions were to rate the video on various aspects for example, if they understood the video and the likelihood of them embracing secure practices.

iii) Additional information-The open-ended questions was used among smartphone users to comment on what they liked and what they did not like about the video.

3.7 Digital Storytelling Framework & Evaluation

This study addressed three objectives:

- i. To investigate information security-related behavior among Kenyan smartphone users.
- ii. To create a Digital Storytelling Model to address information security awareness among Kenyan smartphone users.
- iii. To measure the effectiveness of a digital storytelling model in increasing information security awareness among smartphone users.

3.7.1 User behaviour and their understanding of cybersecurity risks

To understand user behavior when utilizing smartphones, three issues were investigated: (i) security features utilized by smartphone users; (ii) user awareness of potential security threats and (iii) user concerns on security threats. Security measures are features that can be utilized by smartphone users to protect themselves. These features include phone update, phone locking and installing of trusted application prompts among others. This research investigated the security measures which were used by participants in order to identify gaps in the use of security features. To further understand user behavior, participants were asked about their awareness of security threats. The level of user awareness would be useful in creating an effective information security awareness model using digital storytelling.

3.7.2 Digital Storytelling Framework

Table 3.2 shows a summary of the characteristics and processes that are used in this study to design a digital storytelling model (DSM) for increasing cybersecurity awareness among Kenyan smartphone users.

Table 3.2

Characteristics and process framework for designing the digital storytelling model

Type of Digital Story	Characteristics of Digital Story	Process of designing the Model
Information-based	<ul style="list-style-type: none"> a) Author’s point of view b) An important question c) Emotional connection with the audience d) Context e) Soundtrack f) Economy g) Pacing 	<ul style="list-style-type: none"> a) Choose story characters b) Choose story language c) Choose narration style d) Select multimedia elements e) Develop story content f) Create the digital story g) Collect participants’ feedback

(i) The DSM was to inform the viewer (B. R. Robin, 2008).

(ii) The DSM implemented the seven elements contained in digital storytelling (Center for Digital Storytelling, 2005) in the following ways:

- a) point of view, which considered the results of the security features utilized by the users and also their knowledge of security risks and mitigations.
- b) an important question that was to be answered by the end of the narration, which emanated from the most prominent issues that need increased awareness.
- c) emotional content that addresses an issue in a personal way by identifying with the qualities of the study participants.
- d) the gift of voice that contextualizes the story within the Kenyan context.
- e) the use of soundtracks that support the story.
- f) creation of the story within an economical time so as not to overload the viewer.
- g) pacing the story so it neither progresses too slowly or too quickly.

(iii) The DSM followed a process that was used to create digital storytelling by teachers for cyber-risk awareness (Khalid & El-Maliki, 2020). However, these steps did not follow a strict order since some steps work best when completed together.

- a) Chose story characters by considering the background of the respondents involved in this study as well as information security experts.
- b) Chose story language by considering the day-to-day language used by participants involved in this study.
- c) Chose narration style as either first-person or third-person narration.
- d) Selected multimedia elements such as software, soundtrack, images, text, audio.
- e) Developed story content by writing a script. The content related to information obtained on user behaviour and understanding of cybersecurity risks.
- f) Created the digital story that lasts for an economical time.
- g) Measured the effectiveness of the digital story to increase cybersecurity awareness.

3.7.3 Digital Storytelling Evaluation

After the video was created and shared with smartphone users, an evaluation was carried out. All participants who viewed the video were asked to complete a usability questionnaire attached in Appendix 2B. The questionnaire contained 11 questions that borrow from a study that used digital storytelling to

engage children about online privacy (Zhang-Kennedy et al., 2017), with modification to fit information security context in this paper. These questions were:

- a) Demography of the participants in line with the pilot study conducted in this research. This section of the questionnaire was aimed at understanding the characteristics of smartphone users.
- b) Whether or not the participant has prior experience with a digital storytelling media that seeks to increase information on security awareness on the security issue being presented. The answer included yes/no options.

The following aspects of the questionnaire was measured on a scale of 1 to 5, where 1 is least positive and 5 is most positive.

- a) How much fun it was to view the digital storytelling media, in order to test how much participants, enjoy interacting with the digital storytelling media.
- b) How easy it was to understand the video.
- c) How well participants learnt about each metric in the Information Security Belief Model by viewing the digital story.
- d) The potential of behavior changes in relation to using public WiFi after watching the digital story.
- e) The willingness to share the digital story with others.

The following question was open ended.

- a) What the participant liked about the digital story.
- b) What participants did not like about the video.

The data from this evaluation was analyzed using descriptive statistics and presented to show the effectiveness of digital storytelling to increase information security awareness among Kenyan smartphone users.

3.8 Operations Definition of Variables

Dependent and Independent Variables

Table 3.3

Shows the variables in the study

Independent Variable	Dependent Variable
Security Threat Awareness	Digital Storytelling Model (IS Belief Model and Digital Storytelling Framework; Story Creation and Script Content)
Perceived Information Security Risks	
Mobile Information Security Countermeasures	-Increasing Security Awareness -Understanding Security Concepts -Embracing Better Behaviour

The changes in the independent variables, which are Security threat awareness, Perceived information security risks, and Mobile information security countermeasures, affected how the dependent variable which is the Digital storytelling model was designed. Thus, in this study the implementation and evaluation phase (Phase 2) was influenced by the outcome of results from the exploratory pilot phase (Phase 1).

The design of the Digital storytelling model was based on the gaps identified in Phase 1, for example, If the results would depict that users have less knowledge in Security Awareness, DSM created would focus on effective knowledge sharing. On the other hand, If the gap would be on the wrong security choices smartphone users make, the DSM would focus on changing user behaviour in raising awareness. This is because effective user awareness is determined if the informer understand the user, and it should inform as well as influence their behaviour.

The three independent variables contributed in the design of the digital storytelling model. The model was designed using the existing literature and frameworks in digital storytelling with clear story content and script. The resulting model was to effectively raise awareness by increasing improving user understanding security concepts and hence embracing better behaviour.

3.9 Data Analysis

Data analysis is the strategy one intends to use for data analysis (Kumar, 2011). The data collected using the forms were converted to a spreadsheet, which was the main tool for analysis. The data was then cleaned using Microsoft Excel. Data cleaning involved identifying and discarding the inaccurate and incomplete records. The data contained a mixture of qualitative and quantitative data in the form of numbers and also user verbatim feedback. The data from respondents not living in Kenya was discarded because they were out of scope of our target population, hence only analysis of the Kenyan population was performed. Data were then represented through text, graphs and in tabular format.

3.10 Ethical Considerations

Before the study commenced, ethical clearance was obtained from the National Commission for Science, technology and Innovation and Kenya Methodist University Computer Science Department. The ethical clearance is appended in Appendix 1.

In addition, to ensure anonymity of the respondents, the google form did not collect participants personal information such as email address, name or identification number. To also ascertain confidential and integrity of data was preserved, edit rights was not given to participants. Finally, the video participants were chosen on voluntary basis and at the beginning of the research questionnaire, respondents were assured of their privacy.

3.11 Application of PMT and UTAUT to the Methodology

The first research question was motivated by PMT in the sense that it tries to explain behaviour among smartphone user while using their phone. This is in respect to the risks some security practices pose to user, which can lead to user either facing the risk or avoiding it. UTAUT helped in explaining new security features adoption by smartphone users.

In designing the digital storytelling model, which was the second objective, UTAUT and digital storytelling framework played a great role in designing. The model was made to be relatable, hence was preferred by smartphone uses.

Finally, PMT together with UTAUT, contributed significantly in guarging the digital storytelling model effectiveness. This is on effectiveness on security concepts and user like hood of embracing secure behaviour.

CHAPTER FOUR

RESULTS AND DISCUSSION

Data was collected from Kenyan smartphone users in a pilot exploratory phase and also during the implementation and evaluation phase. This chapter presents the results and analyses of these data as per the research process used to address the research questions, namely information-security related behavior, digital storytelling model, and effectiveness of digital storytelling. Appendices 3A and 3B contains the raw data from participants' feedback. First, the following section presents the participants who took part in the study.

4.1 Demographics

4.1.1 Demographics in the Pilot Phase of Study.

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. The responses represented an 83% response rate. The results considered 393 users, who were from Kenya and formed 91 percent of the population as per table 4.1 below.

There was almost a 50-50 representation of male and female participants. 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 per-cent without IT knowledge. Finally, the majority of the participants lived in urban areas and from Kenya. The demographic representation of the participants confirms the ownership of smartphones among a youthful, urban population. The possession of IT knowledge among participants is relevant to this research in relating it to the knowledge and adherence to information security guidelines.

Table 4.1***Smartphone user demographics***

Characteristics	Category	Overall	Percentage
Gender	Male	223	57%
	Female	198	50%
	Prefer not to answer	8	2%
	Not responded	1	0%
Age Group	Less than 20 years	4	1%
	20-30 years	229	58%
	30-40 years	130	33%
	40-50 years	39	10%
	Above 50 years	16	4%
	Prefer not to answer	11	3%
	Not responded	1	0%
Profession	Employed	305	78%
	Student	78	20%
	Retired	1	0%
	Unemployed	37	9%
	No answer	9	2%
Phone Operating System	Android by Google	374	95%
	IOS by Apple	38	10%
	BlackBerry	2	1%
	Windows Phone	3	1%
	I am not Aware	5	1%
	Not responded	8	2%
Phone Monitored by employer	Yes	22	6%
	No	405	103%
	Not responded	3	1%
IT Knowledge	Good	97	25%
	Moderate	173	44%
	Excellent	144	37%
	knowledge	12	3%
	Not responded	4	1%
Settlement Setting	Rural	53	13%
	Urban	372	95%
	Not responded	5	1%
Smartphone Ownership	Yes	429	109%
	No	1	0%
Country	Kenya	393	91%
	Outside Kenya	31	7%
	Not responded	6	1%

4.1.2 Demographics in Evaluation phase of the study.

Questionnaires were sent out by sharing a Google form link via email and WhatsApp. Of the questionnaires sent out, 299 smartphone users responded. The results considered 277 users, who form 93 percent of the population as per table 4.2 below. The 277 responses considered were the respondents from Kenya, as they were the target population.

Table 4.2

Digital Storytelling Model user demographics

Characteristics	Category	Overall	Percentage
Country	Kenya	277	93%
	Outside Kenya	21	7%
	Not responded	1	0%
Settlement Setting	Rural	27	9%
	Urban	272	91%
	Not responded	0	0%
Age Group	20 - 30 years old	125	42%
	30-40 years	135	45%
	40-50 years	15	5%
	Above 50 years	19	6%
	Prefer not to answer	5	2%
	Not responded	0	0%
Profession	Working or Self Employed	242	81%
	Student	37	12%
	Retired	0	0%
	Unemployed	19	6%
	No answer	1	0%
IT Proficiency	Good	91	30%
	Moderate	125	42%
	Excellent	78	26%
	Don't have IT knowledge	5	2%
	Not responded	0	0%
Cities in Kenya	Nairobi City	207	69%
	Iten	1	0%
	Eldoret	21	7%
	Nakuru	3	1%
	Kisumu City	5	2%
	Mombasa City	2	1%
	Other Cities	38	13%

The age group with a higher representation was between the age of 30 and 40 at 45 percent, closely followed by 20-30 years with a percentage of 42 percent. Additionally, 81 percent of the sample were working or self-employed with 12 percent as students. The

participants also displayed good to moderate IT knowledge, with only 2 per-cent without IT knowledge. Finally, the majority of the participants lived in urban area, specifically in Nairobi.

The following sections present the results, per research question.

4.2 What is the information-security related behavior among Kenyan smartphone users?

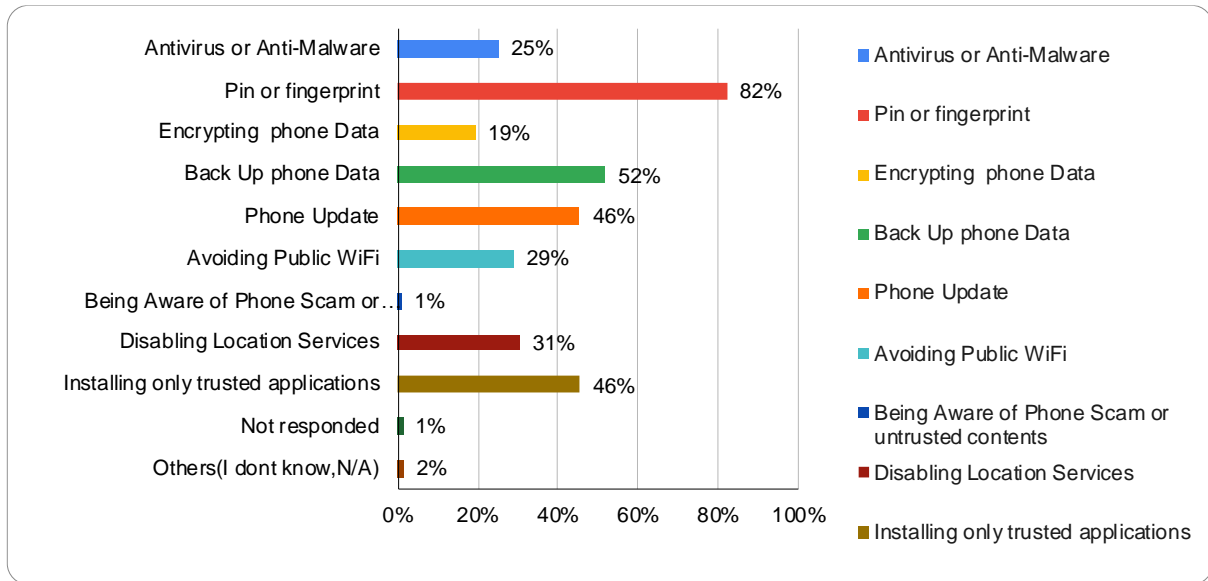
4.2.1 Security features utilized by smartphones users

Figure 4.1 below shows how Smartphone users utilize various security measures in their phones. These features include pin or fingerprint, phone backup, Antivirus use among others.

Figure 4.1 shows that 82% of the respondents utilize pin and fingerprint on their phones, and also 52% back up their data. Utilization of pin and fingerprint may be popular because people often use pin or password to access bank accounts, emails, and mobile service providers. Further, social media, radio, or TV advertisement often remind users of such security measures. 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 et al., 2012). Also, the advertisement by Safaricom, one of Kenyan's telecommunication firm, leading in mobile money market share, emphasizes on the use of voice as subscriber's password to access its services (Safaricom PLC, 2018).

Figure 4.1:

Security features utilized by smartphones users



On the contrary, less than 50% of the participants take security measures. For example, only 29% avoid the use of public unsecured WiFi, only 25% utilize antivirus, and just 19% encrypt their phone data. Also, while almost 50% of the users update their phone's software data and install applications from only trusted sources, they ignore other security measures that could put their information at risk such as enabling their locations services and connecting to public WiFi.

These choices might mean that smartphone users are less aware of these media of data loss, have never experienced data loss through these means or they trust public connections. Further, forgetting to disable locational services might be because most users in this research use android phones, where users do not have options on the use of GPS. Apple, for example, has options of reminding users of the applications using locational 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.

The behavioural gap can be reduced by training as suggested by some of the participants through verbatim feedback:

“Mobile security awareness is key as most users need to know how to protect their devices”

“Kindly let us know what are the best practices for our phone safety”

4.2.2 Antivirus Installation and Use

The research can interpret from **Figure 4.2** and **4.3** below that most smartphone users do not install antivirus on their phones and instead install it on their Personal Computers or Laptops. Lack of antivirus installation on phone might mean that users think that laptops are more vulnerable to attacks than smartphones or that PCs need more protection than the mobile phones.

Figure 4.2:

An illustration of Antivirus use

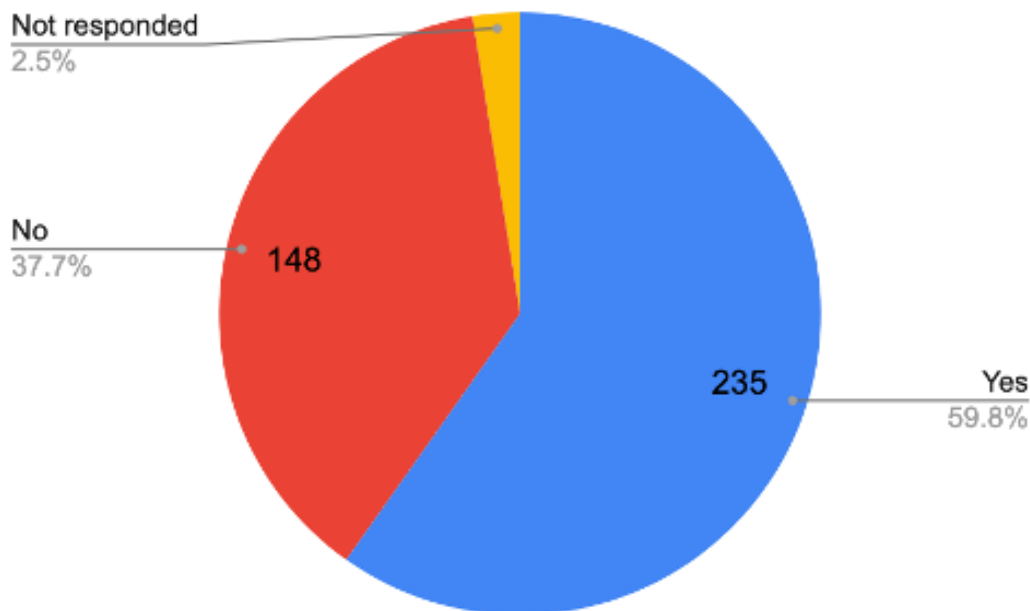
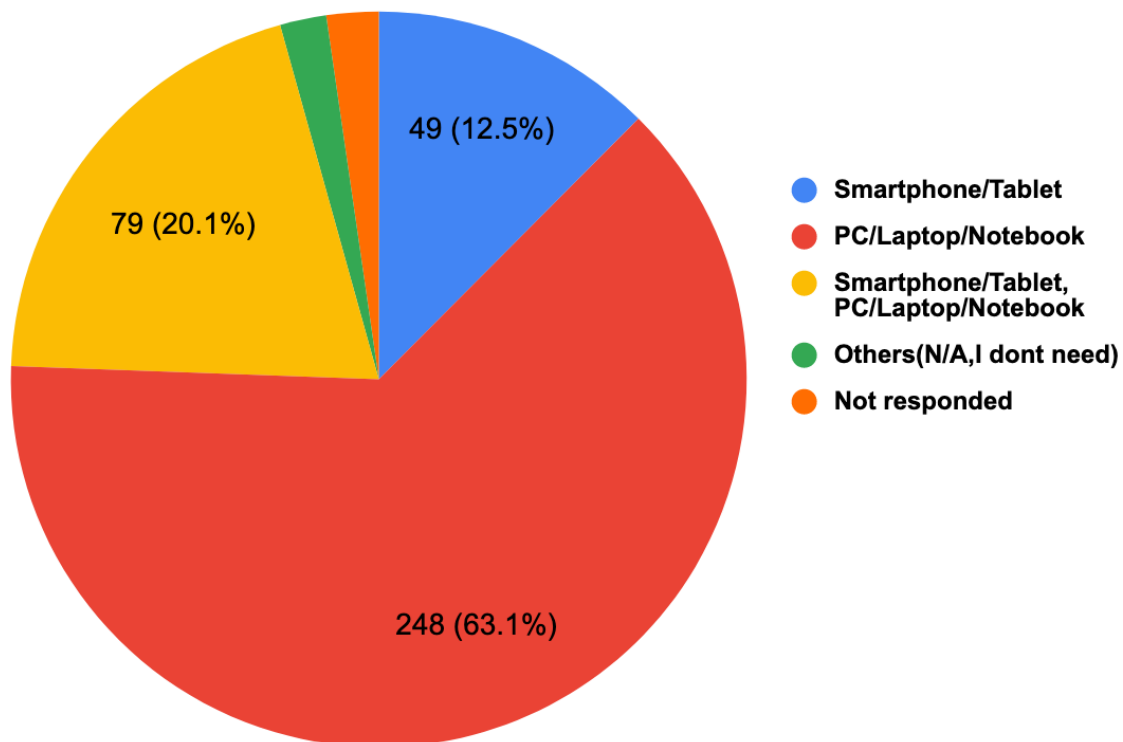


Figure 4.3:

An illustration of Antivirus Installation on Various Gadgets



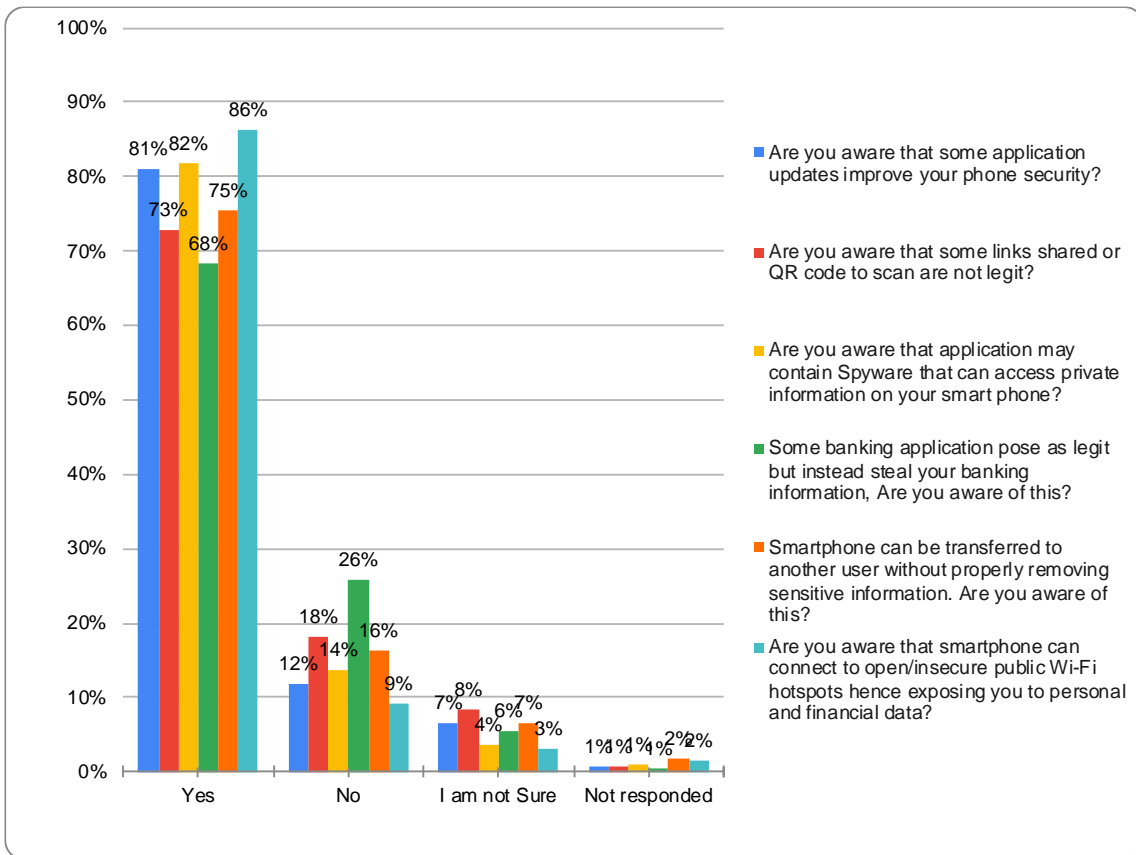
4.2.3 Awareness level of Security Risks

Figure 4.4 below shows that a high number of users are aware that;

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

Figure 4.4:

Awareness level of Security Risks



These findings demonstrate that the awareness level of cybersecurity risk is high as most users are aware of common security risks. Users are generally aware of the most potential threats to their phones. Hence there is an awareness gap on smartphone user’s actions rather than knowledge. For example, users are aware that open public WiFi is risky, yet they still connect to it. in **Figure 4.4**, 81% of users are aware that phone updates improve phone security, on the contrary, in **Figure 4.1** only 46% of users update their smartphone. Likewise, in **Figure 4.4**, 86% of users are aware that open WiFi is risky yet, in Figure 4.1, 71% still connect to it.

4.2.4 User Concern on Information Security Risk

Figure 4.5 below shows that more than 86 percent of smartphone users are concerned to a great extent and to a very great extend about security risk such as;

- i. Some application accessing private information on our phones.
- ii. Spyware accessing information without consent.
- iii. Banking details can be stolen by malicious application.
- iv. Sensitive data might be transferred from one phone owner to another.
- v. Public WiFi can expose personal or financial data.
- vi. Not having a pin or password in a phone.
- vii. Suspicious link or QR codes shared with me.

Furthermore, after users evaluating their concerns on security risk (those described in the above questions), the research asked them if their current level awareness and concern for information security and privacy impact their decision when installing mobile protection on their phones. Similar population proportion, **Figure 4.6**, of those who were greatly concerned about their privacy, 87 percent responded by saying yes. Thus, security risk knowledge greatly influences behaviour. Besides asking the influence of risk on their behaviour, the research also asked them if they thought their level of exposure has influenced the decisions they make, to protect their data on their smartphone. As shown in **Figure 4.7**, 76 Percent, answered yes. User awareness due to exposure suggests that knowledge plays a crucial role in awareness.

Figure 4.5:

User perceived information security risk

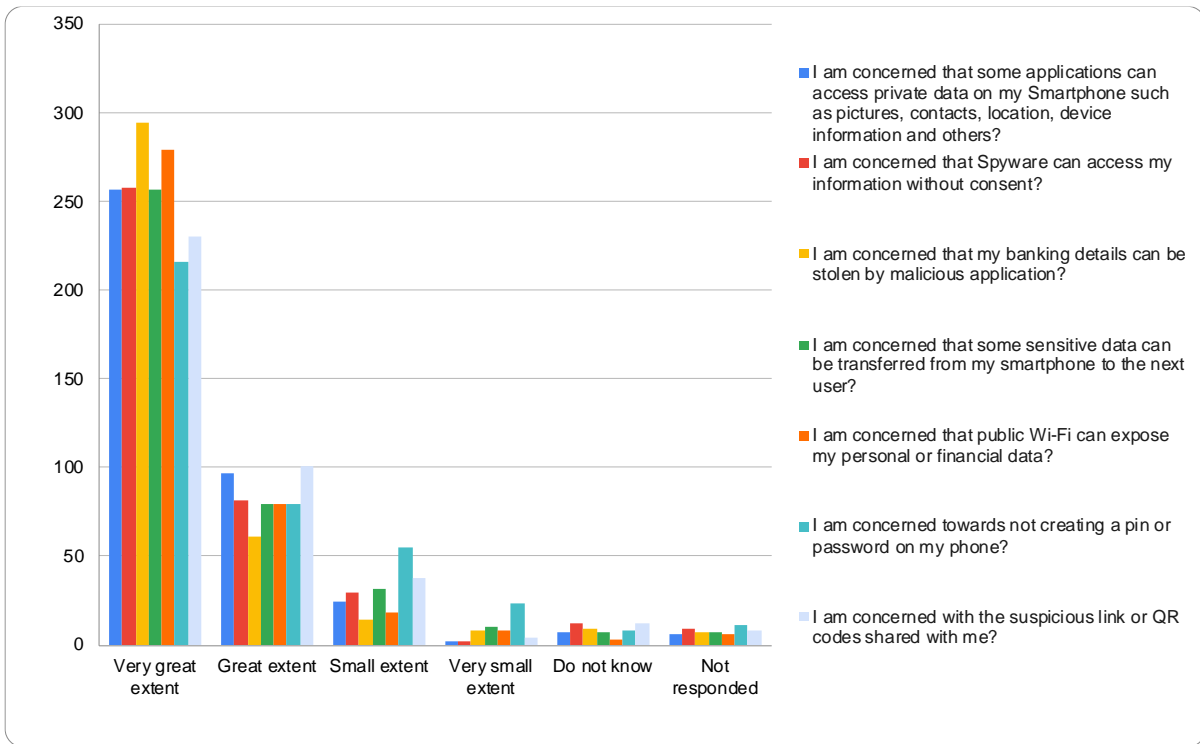


Figure 4.6:

Awareness on risk impacting security decision

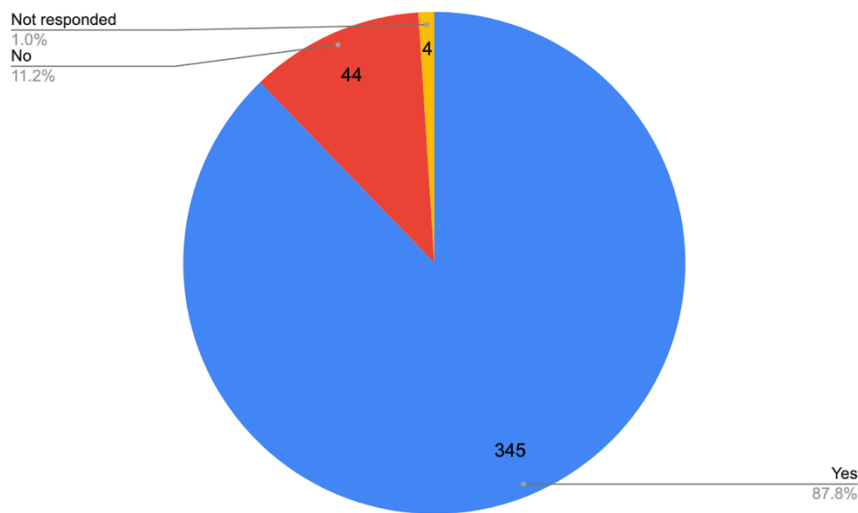
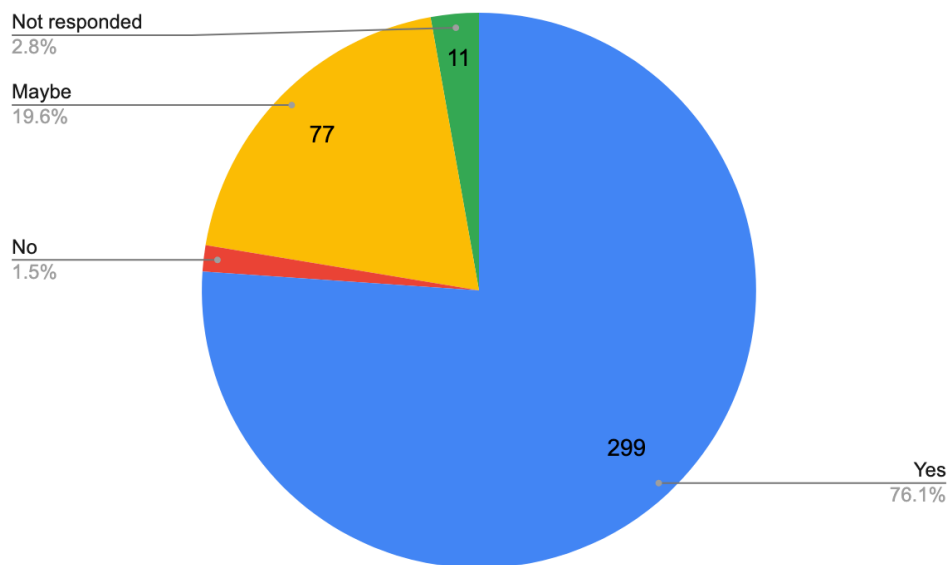


Figure 4.7:

Level of exposure influencing decision



4.2.5 User Security Countermeasures

Not only did the research investigate on user awareness and risk concerns, the research also looked into the measure's smartphone users use to protect themselves from security infringement. The measures include;

1. Where smartphone users get application to install on their phones.

Results revealed that 81 percent of users get applications via official store, **Figure 4.8** i.e., Play Store and Apple Store only. Other sources of application include a mix of the application stores, friends and websites. Installation from less trusted sources reveal that there is a possibility of at least 19 percent of smartphone users installing malicious applications.

2. Factors Smartphone users consider while installing application

There are several factors that smartphone users consider before installing applications. The top three in **Figure 4.9** comprises of user review, familiarity with the brand and popularity. 36 and 32 percent of users considered application permission and application privacy policy

respectively, when installing applications. User choices implies that most users pay less attention to security options during application installation.

Figure 4.8:

Source of mobile applications

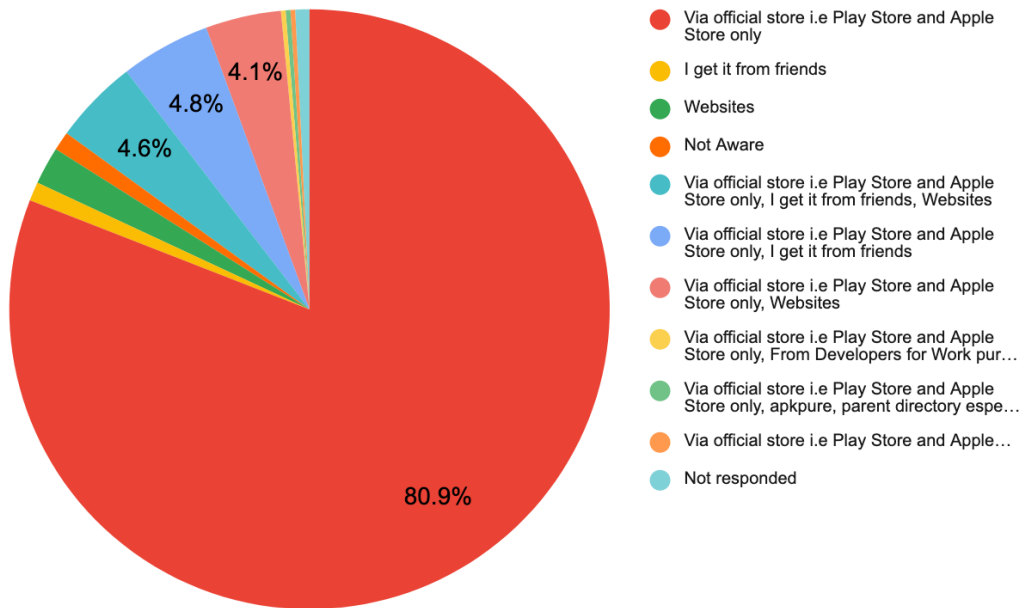
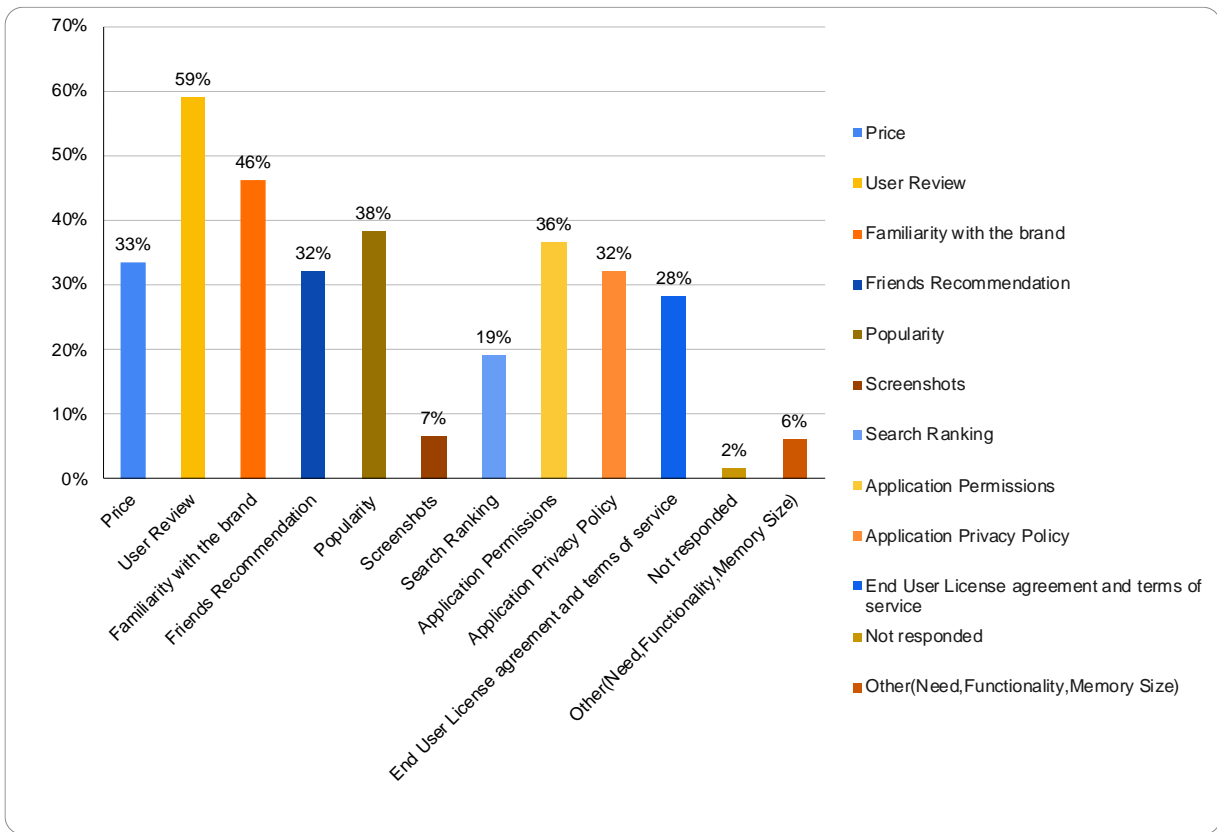


Figure 4.9:

Factors considered while installing an application

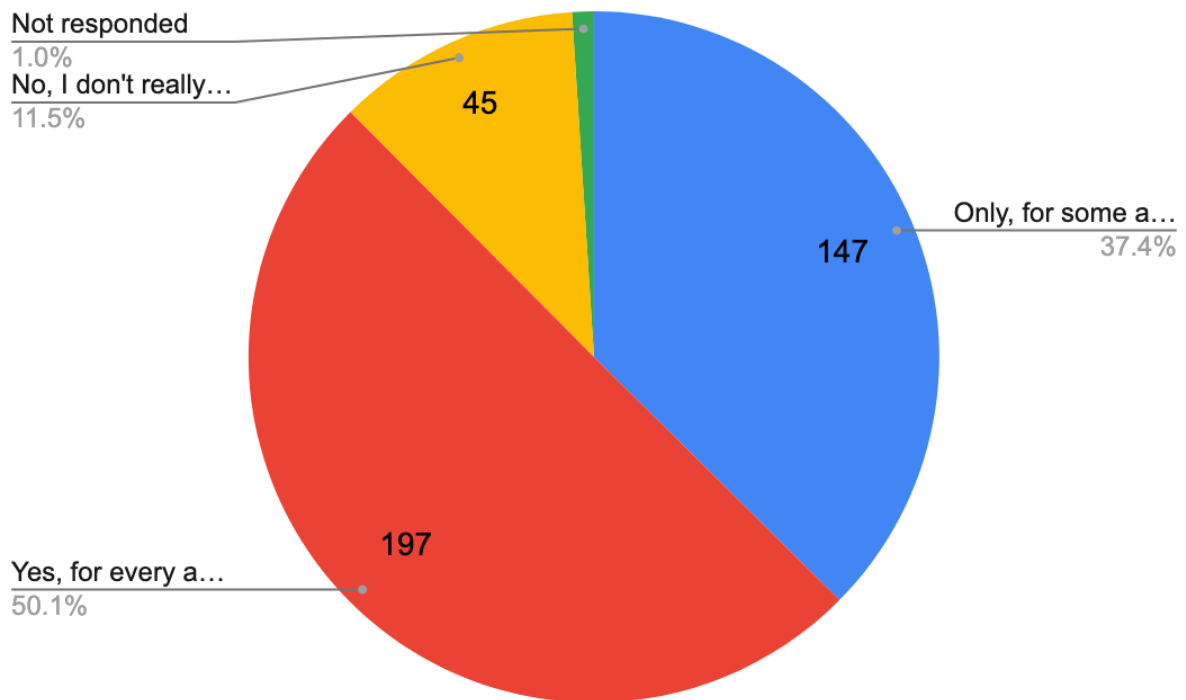


3. Mindfulness of security messages on installation

The research discovered that half of smartphone users pay attention to security messages that appear on their phones during every installation, **Figure 4.10**. The other half are mindful only for some application or they do not really bother. The gap identified on application installation demonstrate a gap that can be addressed.

Figure 4.10:

Mindfulness of security messages during installation

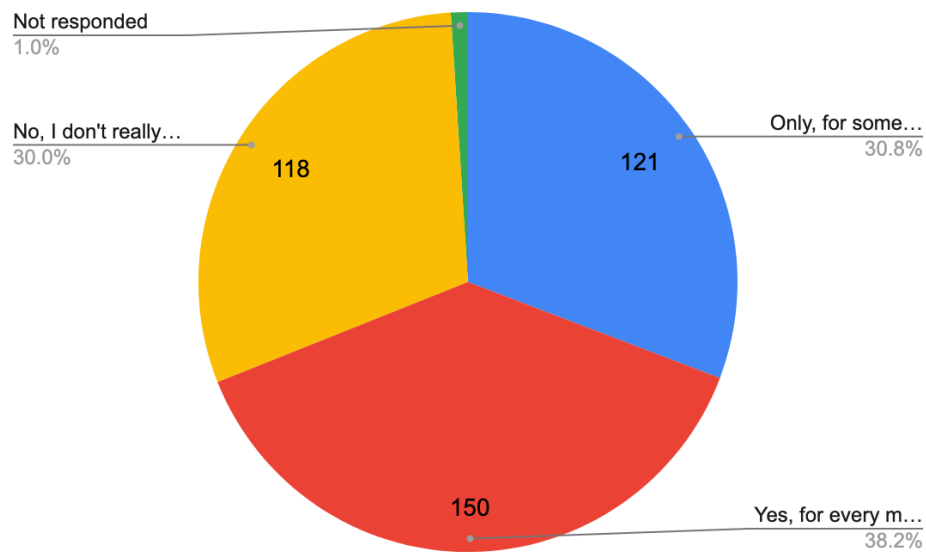


4. Attentiveness to advertisement messages

The research also asked the question on whether smartphone users pay attention to security messages that come to their phone informing them of a promotion or a discount. It was useful to know that more than 60 percent of smartphone users do not heed to security messages that come to their mobile phones, **Figure 4.11**.

Figure 4.11:

Attentiveness to advertisement messages

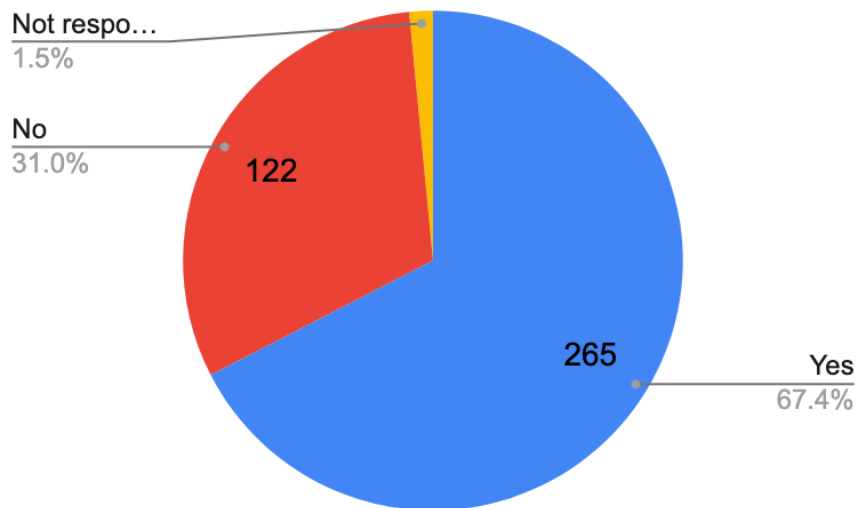


5. Verification of links before opening

The research also made inquiries on whether smartphone users verify links and messages shared before opening. **Figure 4.12** revealed that 67 percent of users verify links, while the remaining do not. Lack of links verification depict that more than 30 percent of users are open to attacks via malicious links.

Figure 4.12:

Link verification before opening

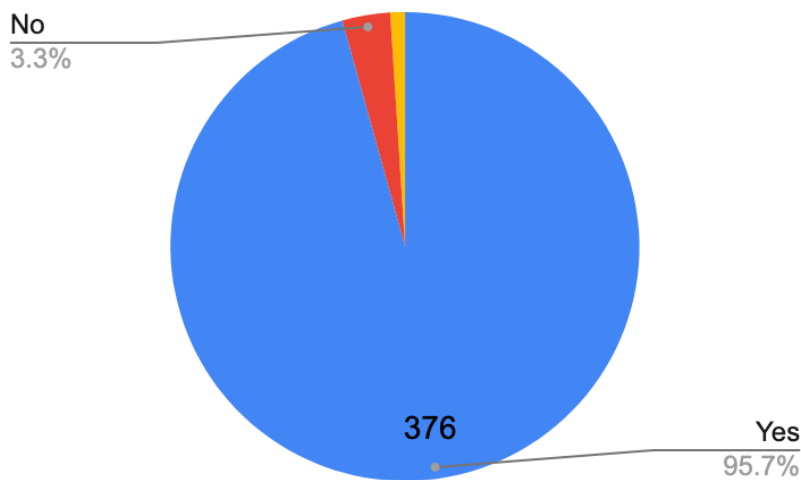


6. Keeping pin and password confidential

On the question of whether users keep pin and password confidential. **Figure 4.13** shows that 96 percent of user keep password confidential. Use of pin and password protection method appears to be the most commonly used as seen in **Figure 4.13**. Hence it is interesting to note that almost all smartphone users keep their pin and password private.

Figure 4.13:

Keeping pins and passwords confidential



4.2.6 Discussion of results to answer Research Question 1

The findings show that Kenyan mobile users are knowledgeable on user security and have great concerns about risks that they are exposed to. However, users still make poor behavioral choices related to the use of smartphones, making them vulnerable to cybersecurity attacks. The gap between user awareness and behavior is similar to the finding on employee's security awareness that showed a difference in employees' knowledge and employee behavior (Workman et al., 2008). The contrast might be because the information security awareness model of a person is based on three metrics: knowledge (what users know), attitude (what users think or feel) and behavior (what users do) (Kruger & Kearney, 2006). Therefore, an impactful information security awareness model is one that is able to build on what users already know and what they think in order to impact behavioral change.

The findings also demonstrate that users' knowledge of security risks alone is not enough to change user behavior. Security behaviour is also influenced by motivation, persuasion, and social norms apart from user knowledge in security (Bada et al., 2015). Thus, an ABC Model

was designed in which employees' attitude towards information security awareness was considered as an issue that is logical and emotional (Saracco, 2008). The model addresses the ABC aspect as follows; A-Emotional aspect of attitude, B- Behavioural component, and C-Cognitive of attitude. Therefore, it is evident that when designing models to increase user information security awareness it is important to consider the difference between what the users know and how they behave.

4.3 What Digital Storytelling Model can be designed to address information security awareness among Kenyan smartphone users?

To answer the second research of this study, this section uses the processes that were displayed in Table 3.2 to design a digital storytelling model, namely the characteristics and process framework for designing the digital storytelling model. This model is a basis for creating digital media for information security awareness among Kenyan smartphone users. In following this process, the model addresses the four major phases cited as a process guide for DST designers: pre-production, production, post-production, and distribution (Hashiroh & Norshuhada, 2016).

4.3.1 Characters

The study findings reveal that the age group with the highest representation at 53 percent was between the age of 20 and 30. From the sample participants, 71 percent of them were either working or self-employed and lived in urban areas in Kenya. Hence by using a character with similar characteristics who is in their twenties, working and living in an urban part of Kenya, the audience is more likely to relate the experiences portrayed to their personal lives with public WiFi use. The seven elements of digital storytelling emphasize the significance of personalizing a digital narrative to help the listeners and viewers better understand the context (Center for Digital Storytelling, 2005).

4.3.2 Language

Kenya is largely multilingual both at the societal and individual levels where an average person speaks at least three languages. However, language structures in the education system identifies English as the main mode of instruction at all levels of education in the urban areas. English is not only dominant in literacy, but also in most public media avenues (Muaka, 2011). Given that 87% of research participants live in an urban setting, and with 96% of them possessing good knowledge in Information Technology, English has been chosen as the language of instruction for the video.

4.3.3 Narration Style

The approach used second-person narration in which, the story was centered on a self-check approach to help audience contemplate to change their behaviour when using public Wi-Fi. The second-person personal pronoun *you* was used by a narrator to identify and directly address a character that represents our audience. The advantage of using a second person point

of view is that the audience, when directly addressed, may feel more intimately involved with the characters and the action in the story (Mildorf, 2016).

4.3.4 Multimedia Elements

a) Software

Adobe Premiere Pro was used to edit the video. It is a timeline-based video editing software application developed by Adobe Systems and published as part of the Adobe Creative Cloud licensing program. Premiere Pro is a comprehensive video editing software application used for editing videos, commercials, film, television, and online video.

b) Soundtrack

In digital stories, when present, the content can be textual, visual or musical, or a combination of these. Before the narrator starts speaking, the story had the music itself set the tone of the narrative. Setting of tone was with music that activated certain associations and feelings to public spaces that provide WiFi. Orientation is the part of the narrative that sets the scene in time or place and introduces the participants involved. The music, together with the narrator's voice have an orientation function. Since the story was told in the second person, the voice introduces the main character. As the story evolves, various musical and sound effects was used in order to signal a change in action. Seeing as the purpose of instructional digital stories is to advise and support, the resolution should be positively encouraging (Bernaerts, 2016). Consequently, the music that matched the resolution was joyful and lively with a rising volume that contributes to this effect.

c) Media

A mixture of visuals, voice narration, and music was used to present a narrative that was overlaid by videos taken on a camera, graphic layouts presenting statistics and instructional

material, and external media such as other videos (B. Robin, 2016). The voice narration was heard at the appropriate volume (without distortion). Reading of the script was expressive, suitably paced, and sufficiently practiced, with no repetition (Campbell, 2012).

4.3.5 Script Content

a) Information Security Issue

Poor behavioural choices regarding security measures among smartphone users increases their risk exposure. The findings indicated that public WiFi is practiced by 71% of participants, locational services enabled by 69% of participants, and 75% of participants were not using antivirus. There is a dire need to urgently address these matters. The proposed model addresses WiFi awareness, given that WiFi is among the top three security threats affecting mobile phones globally (Kaspersky, 2020b).

The WiFi use is growing at unprecedented rate as mobile users are becoming heavy data users and hence WiFi is a cheaper option to use (K. Lee et al., 2013). However, information security belief model can be replicated to raise awareness with other raised issues affecting mobile users.

b) Story Design

c) Information Security Belief Model

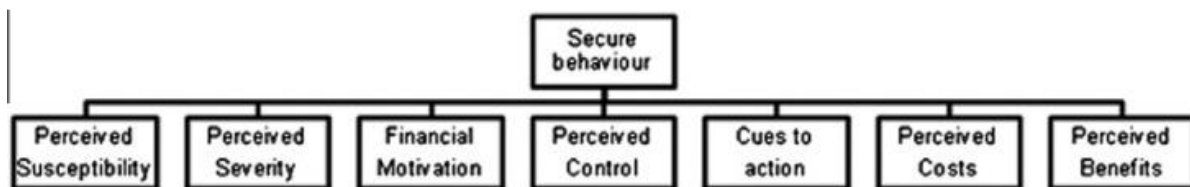
Figure 4.14 shows a process that was proposed to design an awareness model to promote secure behavior among Internet users within the financial sector (Davinson & Sillence, 2010). **Table 4.3** shows how this model has been adapted for this research as an Information Security Belief Model. This process was used to design the digital video.

The first part of the video portrayed the chances of becoming a victim of a public WiFi attack with the aim of increasing susceptibility to the risks involved. Similarly, the second part showcased the consequences of using public WiFi so as to show its severity. The third part

explored if smartphone use are concerned about the use of public WiFi. These first three metrics are aimed at increasing a user’s concern for protecting their information and ultimately motivating them to behave securely when using public WiFi. To further promote safe practices and behavior, the smartphone user is urged to perceive that they can control the occurrence of information security risk, for instance, by switching off automatic connection to public WiFi. Further, the smartphone user must also decide if the perceived benefits outweigh the costs, for instance that switching off automatic connection to public WiFi requires minimal effort and could potentially prevent access to their information without their consent. The smartphone user should then know when to carry out preventive measures so as to protect their information towards the perceived benefits.

Figure 4.14:

Hierarchy of Contributing Factors towards Secure Behavior



Note. (Davinson & Sillence, 2010)

Table 4.3

Adaption of Figure 4.14 to an Information Security Belief Model






Perceived Susceptibility	What are the chances of being a victim of a public WiFi attack?
Perceived severity	How serious are risks involved with public WiFi & their consequences?
Information Security Motivation	Are users concerned that public WiFi can affect their information stored in mobile phones?
Perceived control	Can users prevent attacks from public WiFi by behaving securely?
Cues to action	When should smartphone users behave securely?
Perceived costs	What are the costs of behaving securely?
Perceived benefits	What are the benefits of behaving securely?

d) Storyboard

To implement the information security belief model in Table 4.3, a storyboard was designed as shown in Table 4.4. A storyboard is a textual or a pictorial overview of all of the elements to be included in the digital story. A storyboard is a useful part in the process by enabling organization of the media in a template before the actual creation begins (B. R. Robin & McNeil, 2012). For example, Table 4.4 portrays, using grayscale images, a coffee shop, an airport lounge and a hotel lobby; all being places where a smartphone user may become a victim of a public WiFi attack. Using pictures to represent scenes that was in the video, the storyboard goes on to showcase the dangers inherent with public WiFi and consequences of using it, in order to show its severity.

Table 4.4

Storyboard Illustration for an Information Security Digital Storytelling Model

Multimedia.	Metric from Table 3
<p>Grayscale sketches (Source, Kaspersky- http://alturl.com/s2crz) (Kaspersky, n.d.)</p> 	<p>Portrays the chances of a smartphone user becoming a victim of a public WiFi attack.</p>
	<p>Showcase the consequences of using public WiFi so as to show its severity. Explore whether smartphone users are concerned about the use of public WiFi.</p>
<div data-bbox="197 981 528 1160"> <p>1 AVOID CHECKING SENSITIVE DATA</p> </div> <div data-bbox="555 981 826 1160">  </div> <div data-bbox="879 981 1198 1160"> <p>2 USE A VPN OR HTTPS</p> </div> <div data-bbox="197 1167 596 1335">  </div> <div data-bbox="608 1167 1166 1335"> <p>3 ASK AN EMPLOYEE</p>  </div> <div data-bbox="197 1346 651 1585"> <p>IN KENYA, 86% OF MOBILE PHONE USERS ARE AWARE THAT OPEN PUBLIC WI-FI HOTSPOTS MAY EXPOSE PERSONAL AND FINANCIAL DATA, YET 71% STILL CONNECT TO THEM.</p> </div>	<p>Users perceive they can control the occurrence of information security risk and know when to carry out preventive measures so as to protect their information towards the perceived benefits.</p>
<p>4 NEVER TURN ON AUTO-CONNECT</p>	

e) Script Sample

To implement the storyboard in Table 4.4, and to prepare for the creation of the digital storytelling video, a script was written. **Figure 4.15** shows a sample of the script and **Figure 4.16**, the screenplay.

4.3.6 Story Creation

Economy is mentioned by (Center for Digital Storytelling, 2005) as an important trait of digital storytelling, in that a digital narrative has to use just enough content to tell the story without overburdening the viewer with too much information. Therefore, using the script developed, a digital video was created that lasted between 2 and 5 minutes long (B. Robin, 2016). In the production phase, the steps involved recording a high quality narration of the script, collecting and creating media materials both live with a camera and sourcing footage online, and editing the media materials to form a coherent story.

Figure 4.15:

Script Sample

Script

Picture this. It's Saturday morning and you're hanging out at your local coffee shop using the free Wi-Fi to catch up on a few tasks you couldn't quite get to during your busy week. Sound familiar? This is typical for many of us, but did you know you might be unaware of some threats lurking in the background on public Wi-Fi while you balance your bank account and sip a hot chocolate?

Public Wi-Fi is mostly found in popular public places like airports, coffee shops, malls, restaurants, and hotels — and it allows you to access the Internet for free. Although it sounds harmless to browse some news articles, everyday activities that require a login — like checking your social media account, reading email, or checking your bank account — could be risky business on public Wi-Fi.

Figure 4.16:

Screenplay Sample

FADE IN:

INTERIOR, COFFEE SHOP

Slow motion tracking shot pulling into unoccupied table.

NARRATOR

Picture this. It's Saturday morning and you're hanging out at your local coffee shop using the free Wi-Fi to catch up on a few tasks you couldn't quite get to during your busy week. Sound familiar?

Slow motion pull in to side of subject 1.

SUBJECT 1

Sits with drink and phone in hand. On screen, they scroll through emails. Subject reads one and begins typing a reply.

Camera slow zooms towards phone screen.

The post production phase involved assembling and publishing all the materials. Finally, the video was hosted on a publicly available YouTube channel and shared via a web link (<http://alturl.com/7imq9>) (Hashiroh & Norshuhada, 2016).

4.3.7 Discussion of Results to Answer Research Question 2

The Digital Storytelling Model (DSM) was created by adopting frameworks that have worked in other contexts and inculcating the results drawn from participants of this research. Further, the DSM has been modelled to fulfill all properties recommended for an impactful digital story. The DSM was created by considering criteria in character and language development, narration style, multimedia elements, script content and design, and story creation. In meeting these criteria, the DSM implemented characteristics and frameworks recommended by other researchers. Therefore, the adapted Digital Storytelling Model had the potential of leading to a media that could be effective in increasing information security awareness. The model was then used to design a digital storytelling information security awareness video, which was tested for effectiveness among Kenyan smartphone users.

4.4 What is the Effectiveness of Digital Storytelling in Increasing Information Security Awareness among Kenyan Smartphone Users?

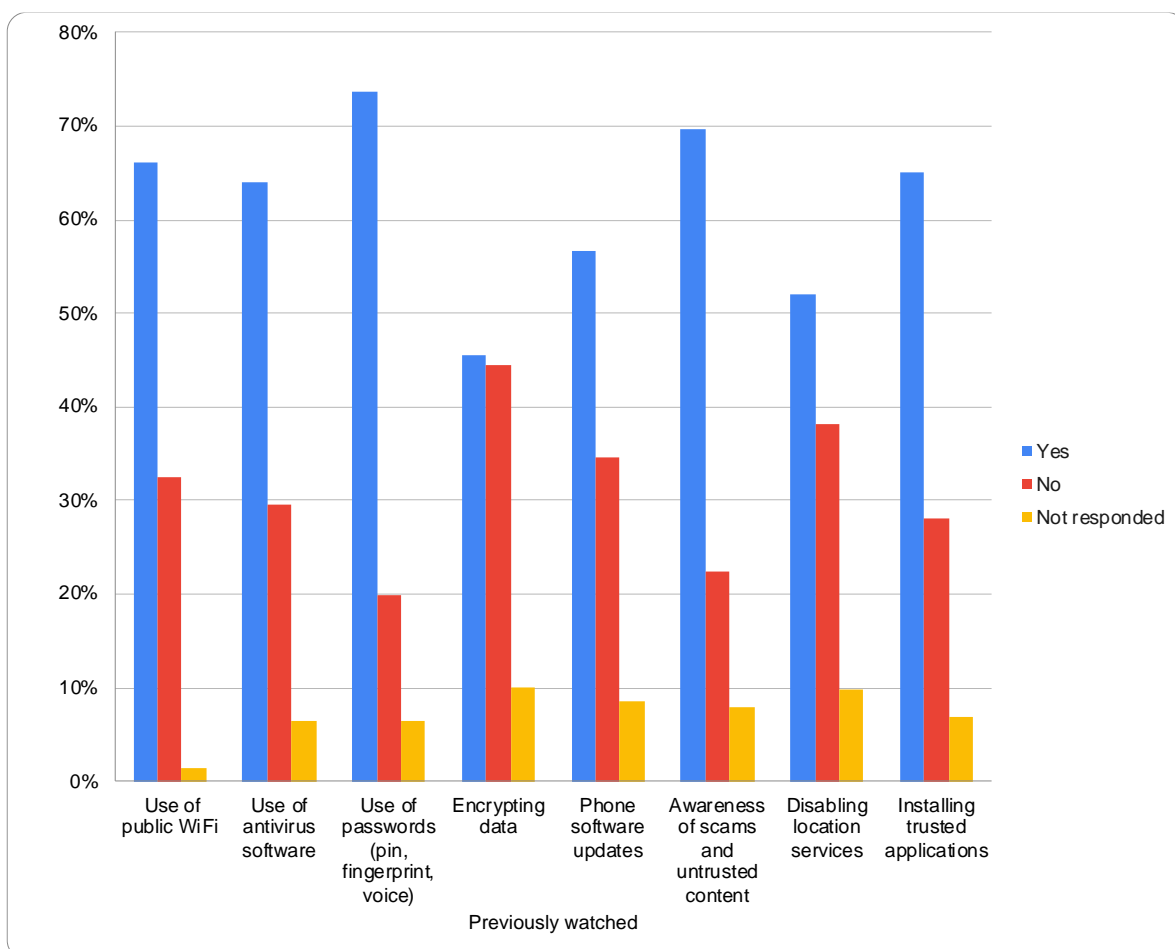
User awareness effectiveness means that digital storytelling would increase knowledge on information security awareness while influencing user behaviour in taking up measures to protect their smartphone data. Digital storytelling effectiveness is reported by: previous experience, quality of video, and impact of video on information security awareness.

4.4.1 Previous Experience in Watching an Awareness Video or Advertisement

To know the user experience in watching an information security awareness video, the research asked questions on various security measures like the use of Pin/Password, use of public WiFi, and use of phone updates. User experience is as shown in **Figure 4.17** below. The results show that an average of 62% among the respondents have watched an information security awareness video or advertisement compared to users who have never watched. The results might be because most media campaigns in Kenya are in the form of print, electronic,

Figure 4.17:

Previous Experience in Watching an Awareness Video or Advertisement



and social media (Okuku et al., 2015). The users have experience in watching awareness video because Safaricom, a mobile telecommunication company in Kenya, run awareness media

targeting its users (Safaricom PLC, 2018). These results could suggest that the media they have watched were not user-centered and highly likely that the impact haven't been measured hence there have been limited user input to the design process of these awareness models.

4.4.2 Video Evaluation

To evaluate how effective the video was, the research asked several questions to rate whether the video was fun, easy to understand and participants' willingness to share the video. The results of the video evaluation are as shown in **Figure 4.18** below. The highly rated aspect of the video was that it was easy to understand, which was strongly agreed on, followed by user willingness to share the video to their network. Finally, 34% and 39% of the users strongly agreed, and agreed that the video was fun, respectively.

Figure 4.18:

Video Evaluation

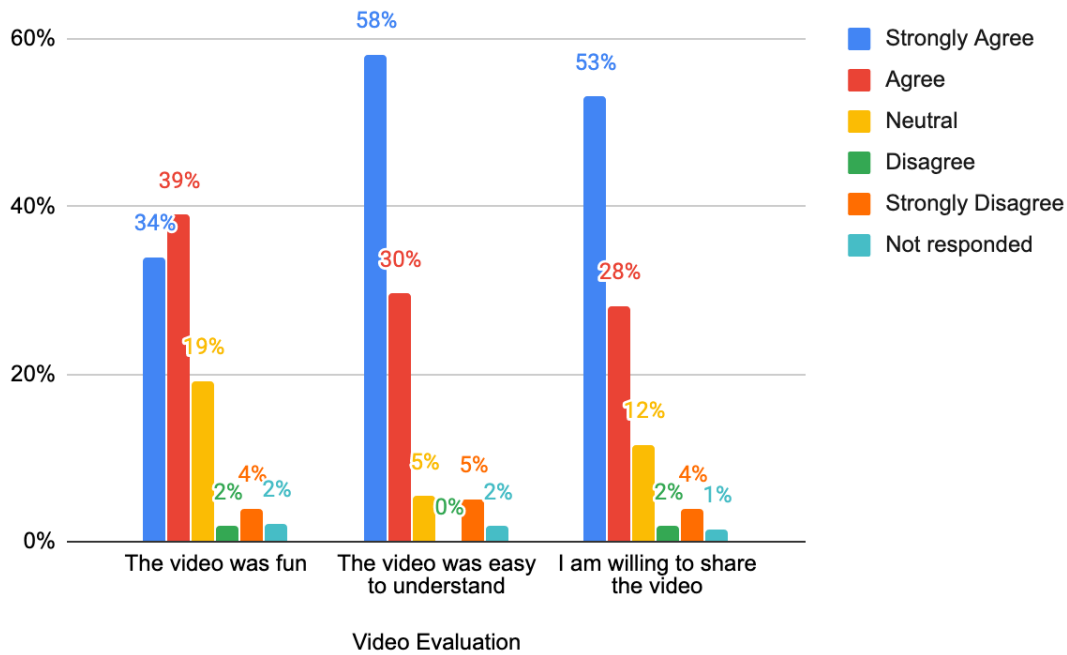


Figure 4.18: Video Evaluation

However, 19 percent of participants rated it as neutral. The neutral results might mean research needs to be explained in-depth, as reflected in a respondent’s verbatim feedback of “Elaborate further”. The fact that most users rated the video as fun, easy to understand and indicated willingness to share meant that the video was of high quality in increasing information awareness about the use of Public WiFi.

4.4.3 Understanding of Security Concepts

The research also sought to understand user knowledge on various security concepts such as the chances of becoming a victim of a public WiFi attack, the risks involved with public WiFi and their consequences, user concern with using public WiFi. Results for security concepts are as shown in **Figure 4.19** below.

Figure 4.19:

User understanding of security Concepts

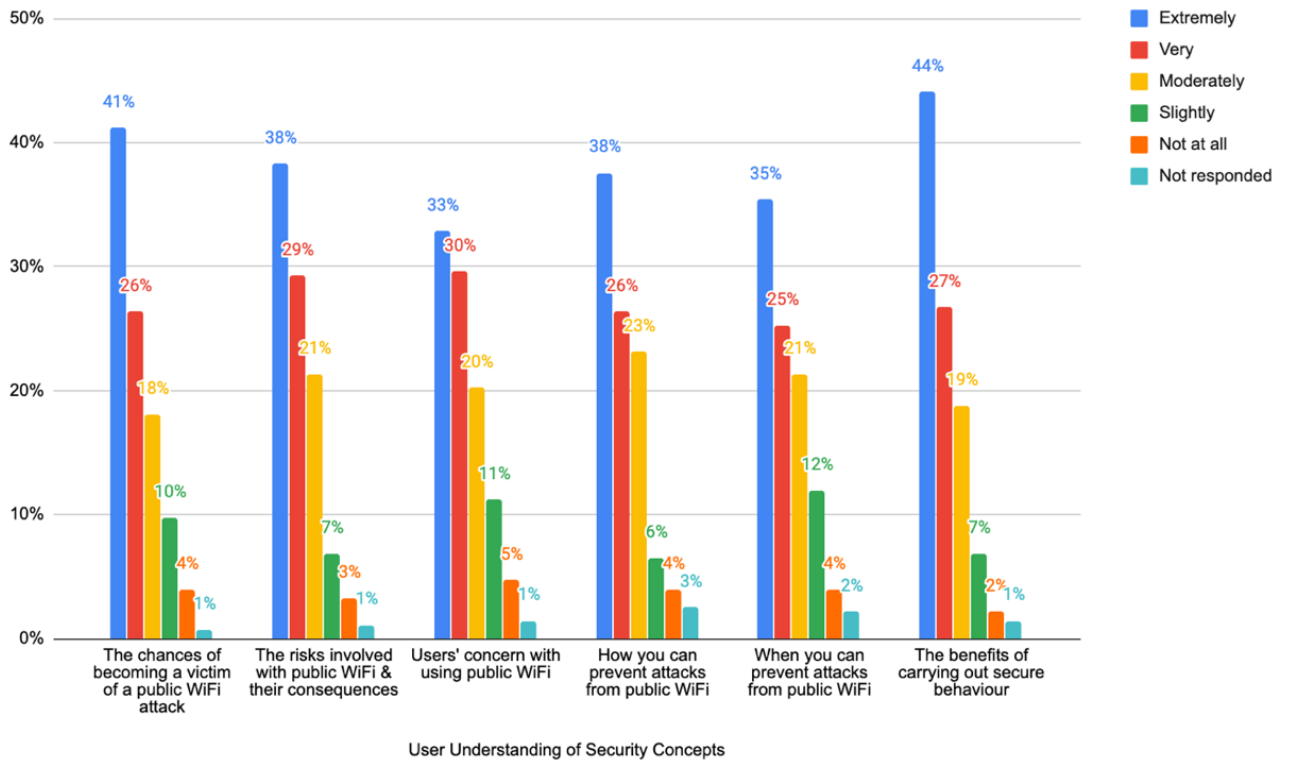


Figure 4.19: User understanding of security Concepts

Figure 4.19 shows that most participants clearly understood all the security concepts by watching the video. An average of 65% indicated that they "Extremely" and "Very" understood all of the concepts by watching the video. In addition, an average of 20% of respondents moderately understood the concepts. These security concepts were the chances of them becoming victims of Public WiFi attacks, the risks involved with using Public WiFi and their consequences, user concerns on using public WiFi, how and when they can prevent attacks from public WiFi and the benefits behaving more securely. These results indicate that the digital storytelling model designed to create the video is impactful in increasing understanding and awareness of security risks.

4.4.4 Likelihood of embracing Secure Practices

To understand the likelihood of embracing secure behaviour among respondents, the research asked users if they would adopt better behaviour. The results of the likelihood of embracing secure behaviour is as shown in **Figure 4.20** below. **Figure 4.20** shows that an average of 52% percent of users are very likely to adopt secure behavior after watching the video. Also, an average of 18 percent of users are likely to adopt secure behavior after watching the video. These results demonstrate that the designed Digital Storytelling Model is highly effective in changing user attitude and belief and consequently behaviour.

4.4.5 Verbatim Feedback from Watching the video

The following positive feedback was received from the respondents:

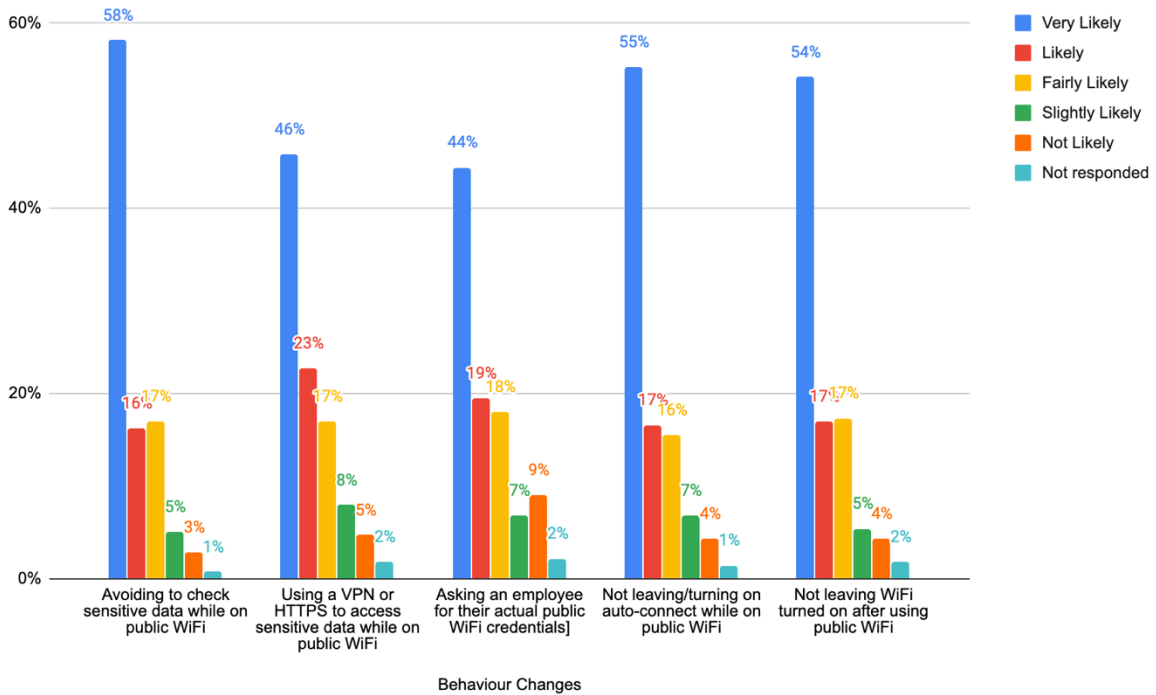
“It was educative and gives clear information on the risks of using public WiFi”

“Simple, easy to understand, use of an everyday situation to explain a technical thing.”

“It was very engaging and clear on what it was meant to address”

Figure 4.20:

Likelihood of embracing secure practices



“The setting...coffee shop, the way descriptive language was used to explain stuff”

“The clarity and ease of explanation to laymen regarding cyber security. It breaks down a complex topic in an easy to understand way”

“It was generally very creative. I highly recommend more if such videos to create awareness on various online security threats”

“It describes complex IT concepts in a very simple manner, I look forward to reading the full paper.”

“The simplicity of delivery and informativeness of the video.”

“The video has given me an alert on public WiFi uses which I didn’t know.”

These positive results further indicate the impact of digital storytelling in increasing information security awareness among smartphone users.

The following negative feedback were received from respondents;

“Short”

“Elaborate further”

“I want to learn more about using a vpn”

“Some terms were complex. I didn't understand all the terms.”

“Felt slow”

“The speed. But that's a personal preference... because well my concentration span is very limited”

“It is very fast”

These feedbacks indicate that there is need for further information security awareness on various topics. Also, they provide an avenue for future work that could test the effectiveness of the length of the video, pace of the video and add more local content.

4.4.6 Discussion of Results to Answer Research Question 3

To address the behavioural gap in user information awareness, this thesis proposed and tested the use of a digital storytelling model to increase cybersecurity awareness among smartphone users in Kenya. Despite the fact that participants had watched other awareness videos and advertisement, there is a high likelihood that user will embrace better behavior if digital storytelling model is adopted as a mode of security awareness. Digital storytelling is very effective in raising user awareness and impacting behavioural change because it brings clarity to the smartphone user, makes it easy to understand the concepts in a fun way hence having the potential of being remembered for long.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

The proposition of this research was that digital storytelling could be an effective mode to increase information security awareness among Kenyan smartphone users, and also influence their security-related behavior towards positive change. To address this proposition, three research questions were posed:

- i. What is the information security-related behavior among Kenyan smartphone users?*
- ii. What Digital Storytelling Model can be designed to address information security awareness among Kenyan smartphone users?*
- iii. What is the effectiveness of Digital Storytelling in increasing awareness of information security among Kenyan smartphone users?*

This chapter begins with a summary of how the results addressed the research questions, and the drawn conclusion. Finally, the chapter discusses the recommendations from the study and suggestions for future work.

5.1 Summary

The research questions of this research were:

- i. What is the information security-related behavior among Kenyan smartphone users?
- ii. What Digital Storytelling Model can be designed to address information security awareness among Kenyan smartphone users?
- iii. What is the effectiveness of Digital Storytelling in increasing awareness of information security among Kenyan smartphone users?

To answer the first research question, the research found out that there is a behavioural gap among Kenyan smartphone users, hence users need more than information. Thus, there

was a need for a human-centered solution that not only raises awareness but also changes behaviour.

To answer the second research question, a digital story telling model was designed from various tested frameworks into an information security belief model. This model was then followed to design a video as a media of storytelling.

To answer the third research question, the Digital storytelling model (DSM) was tested for effectiveness by surveying smartphone users. The results indicate that digital storytelling was highly effective among an average of 65% of the participants in increasing the understanding of risks and secure behavior related to the use of public Wi-Fi. Further, the outcome indicates that an average of 70% of the participants had a high likelihood of adapting security-related behavior as a result of watching the video. Hence DSM is an effective method of raising information security awareness among Kenyan smartphones users.

5.2 Conclusion

The finding shows that Kenyan smartphone users are knowledgeable on security measures available to them. However, they still behave in a way that leaves them vulnerable to mobile security threats. Therefore, user awareness should not only provide information to users but address behavioural gap, that is, what users are doing. The awareness should be targeted, actionable, doable and provide feedback. The Digital Storytelling Model (DSM) is proposed to increase awareness among users and also change their behaviour. The DSM model was created by adopting frameworks that have worked in other contexts and inculcating the results drawn from participants of phase 1 of this research. Further, the DSM model was modelled to fulfill all properties recommended for an impactful digital story. The model was a prelude to a digital storytelling information security awareness video, which was tested for effectiveness among Kenyan smartphone users.

The results showed that smartphone users are highly likely to embrace better behaviors if digital storytelling model is adopted in security awareness, consequently, filling the behavioural gap identified. There is a likelihood of embracing better security measures due to DSM because it is clear, fun, and easy to understand, hence having the potential of improving engagements and knowledge retention.

5.3 Recommendations for Further Research

This study has paved the way for the following areas that can be explored by future research.

i) Exploration of user needs in rural areas

The participants in this study were mostly from urban areas, as demonstrated by the demographics. Thus, future work can explore the information-security behavior among users in rural areas, and subsequently, their needs in an awareness model.

ii) Digital Storytelling for other security issues

This study used the issue of 'Public WiFi' to show the effectiveness of Digital Storytelling. Thus, Digital Storytelling can be tested further with other security issues.

iii) Comparison of Digital Storytelling with other media

This study focused on use of Digital Storytelling to increase information security awareness among smartphone users. Thus, future work can compare the effectiveness between Digital Storytelling and other modes such as SMS-based awareness or social media awareness.

5.4 Recommendations on Research Findings

The findings from this study led to the following recommendations.

i) Design of Information-Security Awareness Media

It is recommended that information service providers and security agencies include user needs and feedback when designing security awareness media. This process could lead to impactful media that results in behavior change.

ii) Implementing Secure Behavior when using Mobile Phones

The following recommendations are given to smartphone users:

- a. Users to disable GPS after use and to keep their phone IMEI number with them.
- b. Smartphone users ought to install antivirus on their phones just like they install it on their Personal Computers, encrypt their phone data and pay more attention to phone security options during application installation.
- c. Users to pay attention to security messages that appear on their phones during every installation and smartphone users to heed to security messages that come to their mobile phones informing them of promotions and discounts.

iii) Regulation of Mobile Applications

It is recommended that applications be regulated, and apps be ranked based on user security. In addition, software developers should develop more apps where by default the user data is protected. As a user suggested “You help us to protect our privacy”.

5.5 Published Papers and Conferences from this Thesis

Journal Articles

- i) Lynet, K., Mbogo, C., & Mwaniki, N. (2020). A Digital Storytelling Model for Increasing Information Security Awareness among Kenyan Smartphone Users. *International Journal of Professional Practice*, 8(1), 92-104. Retrieved from <http://library.kemu.ac.ke/ijpp/index.php/ijpp/article/view/56>
- ii) Lynet, K., Mbogo, C., & Munene, D. (In Press). Relationship between the Behavior of Kenyan Smartphone Users and Awareness of Information Security Practices. *Lukenya University Journal*

Conferences

- i) Lynet, K., Mbogo, C., & Munene, D. (2020, July 24). Relationship between the Behavior of Kenyan Smartphone Users and Awareness of Information Security Practices. *Lukenya University First web Conference series*. Nairobi, Kenya.

REFERENCES

- Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing*, 31(2), 96–110. <https://doi.org/10.1080/08911762.2017.1412552>
- Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science*, 72, 361–373. <https://doi.org/10.1016/j.procs.2015.12.151>
- Ali, A. (2017). Ransomware: A Research and a Personal Case Study of Dealing with this Nasty Malware. *Issues in Informing Science and Information Technology*, 14, 087–099. <https://doi.org/10.28945/3707>
- Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*, 12(3), 1–35. <https://doi.org/10.1371/journal.pone.0173284>
- Androulidakis, I. I. (2016). Mobile phone security and forensics: A practical approach, second edition. In I. Androulidakis *Mobile Phone Security and Forensics: A Practical Approach* (2nd ed., pp 87-109). Springer. <https://doi.org/10.1007/978-3-319-29742-2>
- Apple Inc. (2018). *iOS Security iOS 12*. White Paper. https://www.apple.com/cn/business/docs/site/iOS_Security_Guide.pdf
- Arsenijevic, O., Trivan, D., & Milosevic, M. (2016). Storytelling as a modern tool of construction of information security corporate culture. *Ekonomika*, 62(4), 105–114. <https://doi.org/10.5937/ekonomika1604105a>
- Arshad, S., Ali, M., Khan, A., & Ahmed, M. (2016). Android Malware Detection & Protection: A Survey. *International Journal of Advanced Computer Science and Applications*, 7(2), 463–475. <https://doi.org/10.14569/IJACSA.2016.070262>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015, February 26-27). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* [conference Session] International Conference on Cyber Security for Sustainable Society, Coventry, United Kingdom. <http://arxiv.org/abs/1901.02672>
- Bernaerts, L. (2016). Voice and Sound in the Anti-Narrative Radio Play. In Mildorf/Kinzel (Ed.), *Audionarratology* (pp. 133–158). De Gruyter. <https://doi.org/10.1515/9783110472752>
- Bromberg, N. R., Techatassanasoontorn, A. A., & Diaz Andrade, A. (2013). Engaging Students: Digital Storytelling in Information Systems Learning. *Pacific Asia Journal of the Association for Information Systems*, 5(1), 1–22. <https://doi.org/10.17705/1pais.05101>
- Campbell, T. A. (2012). Digital Storytelling in an Elementary Classroom: Going Beyond Entertainment. *Procedia - Social and Behavioral Sciences*, 69, 385–393. <https://doi.org/10.1016/j.sbspro.2012.11.424>
- Center for Digital Storytelling. (2005). *StoryCenter*. <https://www.storycenter.org/>
- Chaplin, M., & Creasey, J. (2011). The 2011 Standard of Good Practice Principal. *Information Security Forum*, June, 292. [www.securityforum.org](http://www.securityforum.org/web/www.securityforum.org)
- Check Point Software Technologies LTD. (2020). *Live Cyber Threat Map Check Point*. <https://cybermap.kaspersky.com/stats>
- Communications Authority of Kenya. (2018). *Fourth Quarter Sector Statistics Report for the Financial Year 2017/2018 (April-June 2018)*. Communications Authority of Kenya. <https://ca.go.ke/wp-content/uploads/2018/10/Quarter-Four-sector-statistics-report-for-the-Financial-Year-2017-18.pdf>
- Conner, N. (1996). *The role of social cognition in health behaviours*. Predicting Health

- Behavior. <https://psycnet.apa.org/record/1996-97268-001>
- Corley, K. G., & Gioia, D. A. (2011). Building theory about theory building: what constitutes a theoretical contribution? *Academy of Management Review*, 36(1), 12–32. <https://doi.org/10.5465/AMR.2011.55662499>
- Cukier, M., Maimon, D., & Berthier, R. (2012). *A journey towards rigorous cybersecurity experiments*. <https://doi.org/10.1145/2379616.2379620>
- Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. *Information and Computer Security*, 24(1), 116–134. <https://doi.org/10.1108/ICS-04-2015-0018>
- Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, 26(6). <https://doi.org/10.1016/j.chb.2010.06.023>
- Dimensional Research. (2017). *The growing threat of mobile device security breaches the growing threat* www.dimensionalsearch.com
- ENISA. (2010). *The new users' guide: How to raise information security awareness (EN)*. Information Security. https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide
- Escobar-Rodríguez, T., & Carvajal-Trujillo, E. (2014). Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model. *Tourism Management*, 43, 70–88. <https://doi.org/10.1016/j.tourman.2014.01.017>
- Farmer, M. Y., Liu, A., & Dotson, M. (2016). Mobile Phone Applications (WhatsApp) Facilitate Communication Among Student Health Volunteers in Kenya. *Journal of Adolescent Health*, 58(2), S54–S55. <https://doi.org/10.1016/j.jadohealth.2015.10.121>
- Ferrara, E. La, Chong, A., & Duryea, S. (2012). Soap Operas and Fertility: Evidence from Brazil. *American Economic Journal: Applied Economics*, 4(4), 1–31. <https://doi.org/10.2139/ssrn.1820921>
- Fincher, M., & Hadnagy, C. (2015). *The DEF CON 23 Social Engineering Capture the Flag Report*. https://www.social-engineer.org/wp-content/uploads/2015/11/SECTF-2015_Public.pdf
- Giles, H., & Marnix, D. (2010). Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency*, 710(1), <https://ifap.ru/library/book487.pdf>. <https://ifap.ru/library/book487.pdf>
- Gkioulos, V., Wangen, G., & Katsikas, S. K. (2017). User modelling validation over the security awareness of digital natives. *Future Internet*, 9(3), 1–16. <https://doi.org/10.3390/fi9030032>
- Hashiroh, H., & Norshuhada, S. (2016). A Digital Storytelling Process Guide for Designers. *Journal of Telecommunication, Electronic and Computer Engineering*, 8(8), 13–17. <https://doi.org/http://journal.utem.edu.my/index.php/jtec/article/view/1312>
- Honan, M. (2016). *How Apple and Amazon Security Flaws Led to My Epic Hacking*. In *The Best Business Writing 2013*. <https://doi.org/10.7312/star16075-030>
- Iqbal, M., Nisha, N., & Rifat, A. (2018). E-Government Service Adoption and the Impact of Privacy and Trust. In *Encyclopedia of Information Science and Technology*, (4th ed., pp. 3579–3590). IGI Global. <https://doi.org/10.4018/978-1-5225-2255-3.ch311>
- Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. *Information Technology for Development*, 20(2), 196–213. <https://doi.org/10.1080/02681102.2013.814040>
- Jiang, M., Tsai, H. yi S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices.

- Educational Gerontology*, 42(9), 621–634.
<https://doi.org/10.1080/03601277.2016.1205408>
- Jidiga, G. R., & Sammulal, P. (2013, July 4-6). *The need of awareness in cyber security with a case study*. Fourth International Conference on Computing, Communications and Networking Technologies, (ICCCNT), Tiruchengode, India
<https://doi.org/10.1109/ICCCNT.2013.6726789>
- Jumia. (2019). *Kenya Mobile Report 2019*. <https://www.jumia.co.ke/sp-mobile-report/>
- Kaspersky. (n.d.). *Security Dangers of Public Wi-Fi - YouTube*.
<https://www.youtube.com/watch?v=XcghUy-8VRA>
- Kaspersky. (2020a). *Kaspersky Cyberthreat real-time map*. Kaspersky Cyberthreat Real-Time Map. <https://cybermap.kaspersky.com/stats>
- Kaspersky. (2020b). *Top 7 Mobile Security Threats in 2020*. Kaspersky.
https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store?campaign=tcid_admitad_6ab325772c71d0e99b5c5a2683dc3a2e_240682_x4&ADDITIONAL_reseller=tcid_adm
- Kenya National Bureau of Statistics. (2019). 2019 Kenya Population and Housing Census Volume 1: Population by County and Sub-County. In *2019 Kenya Population and Housing Census: Vol. I* (Issue November). <https://www.knbs.or.ke/?wpdmpro=2019-kenya-population-and-housing-census-volume-i-population-by-county-and-sub-county>
- Khalid, F., & El-Maliki, T. (2020). Teachers experiences in the development of digital storytelling for cyber risk awareness. *International Journal of Advanced Computer Science and Applications*, 11(2), 186–191. <https://doi.org/10.14569/ijacsa.2020.0110225>
- Kiboi, N. (2015). *Cyber Security as an Emerging Threat to Kenya Security* [Doctoral dissertation, University of Pretoria]. <https://repository.up.ac.za/handle/2263/50644>
- Kothari, C. R. (2004). *Research Methodology Methods and Techniques*. (2nd ed.) New Age International (P) Ltd <https://doi.org/10.1017/CBO9781107415324.004>
- 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>
- Kumar, R. (2011). *Research Methodology: A step-by-step guide for beginners*. (3rd ed.). Sage Publications, Inc.
<https://doi.org/http://196.29.172.66:8080/jspui/bitstream/123456789/2574/1/Research%20Methodology.pdf>
- 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/10.1080/01449290600879344>
- Lee, K., Lee, J., Yi, Y., Rhee, I., & Chong, S. (2013). Mobile data offloading: How much can wifi deliver? *IEEE/ACM Transactions on Networking*.
<https://doi.org/10.1109/TNET.2012.2218122>
- Leong, Q. L., & Karim, S. (2015). Global perspective in tourism development: Positioning Malaysia as a culinary destination. In *Handbook of Research on Global Hospitality and Tourism Management* (pp. 406–439). IGI Global. <https://doi.org/10.4018/978-1-4666-8606-9.ch021>
- Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, 20, 84–89.
<https://doi.org/10.1016/j.jisa.2014.11.001>
- Martin, J. (2014). *Cybersecurity Awareness Is About Both 'Knowing' and 'Doing'.* Security Intelligence. <https://securityintelligence.com/cybersecurity-awareness-is-about-both->

knowing-and-doing/

- Mataracioglu, T., & Ozkan, S. (2011). *User awareness measurement through social engineering*. August, arXiv preprint arXiv:1108.2149. <http://arxiv.org/abs/1108.2149>
- Mathisen, J. (2004). *Measuring Information Security Awareness. A survey showing the Norwegian way to do it*. [Masters Thesis, Stockholms University] <http://hdl.handle.net/11250/143904>
- Mildorf, J. (2016). Reconsidering second-person narration and involvement. *Language and Literature*, 25(2), 145–158. <https://doi.org/10.1177/0963947016638985>
- Muaka, L. (2011). Language Perceptions and Identity among Kenyan Speakers. In M. C. P. P. Somerville (Ed.), *In Selected Proceedings of the 40th Annual Conference on African Linguistics* (pp. 217–230). Somerville, MA: Cascadilla Proceedings Project.
- Mugenda, O. M. M. & A. G. (1999). *Research Methods: Quantitative & Qualitative Approaches*. Acts press.
- Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers and Security*, 34, 47–66. <https://doi.org/10.1016/j.cose.2012.11.004>
- Nassuora, A. (2013). Students Acceptance of Mobile Learning for Higher Education in Saudi Arabia. *International Journal of Learning Management Systems*, 1(1), 1-9 <https://doi.org/10.12785/ijlms/010101>
- Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybers Security Strategy's Role in Raising Kenyan Awareness of Mobile Security Threats. *Okuku, Renaud & Valeriano*, 32, 1–20. <https://doi.org/http://dx.doi.org/10.11610/isij.3207>
- Oladipo, T. (2015). *Cyber-crime is Africa's "next big threat", experts warn - BBC News*. <https://www.bbc.com/news/world-africa-34830724>
- Ophoff, J., & Robinson, M. (2014, August 13-14). *Exploring end-user smartphone security awareness within a South African context*. [conference Session] Information Security for South Africa ISSA Conference Johannesburg, South Africa <https://doi.org/10.1109/ISSA.2014.6950500>
- Osborn Quarshie, H., & Martin- Odoom, A. (2012). Fighting Cybercrime in Africa. *Computer Science and Engineering*, 2(6), 98–100. <https://doi.org/10.5923/j.computer.20120206.03>
- Parker, F., Ophoff, J., Van Belle, J. P., & Karia, R. (2015, November 15-17). *Security awareness and adoption of security controls by smartphone users*. [conference Session] Second International Conference on Information Security and Cyber Forensics, (InfoSec), Cape Town, South Africa <https://doi.org/10.1109/InfoSec.2015.7435513>
- Paul, W., Ben, N., Kavitha, C., Scott, W., & Kevin, H. (. (2016). Symantec Internet Security Threat Report 2015. In *Internet Security Threat Report*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf
- Pew Research Center. (2015). *Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations. Numbers, Facts and Trends Shaping the World*, 1–75. <https://www.pewresearch.org/global/2015/03/19/internet-seen-as-positive-influence-on-education-but-negative-influence-on-morality-in-emerging-and-developing-nations/>
- Rader, E., Wash, R., & Brooks, B. (2012). *Stories as informal lessons about security*. In Proceedings of the Eighth Symposium on Usable Privacy and Security, 1–17. <https://doi.org/10.1145/2335356.2335364>
- Raghuramu, A., Zang, H., & Chuah, C. N. (2015). Uncovering the footprints of malicious traffic in cellular data networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-15509-8_6


- Robin, B. (2008). Digital storytelling: A powerful technology tool for the 21st century classroom. *Theory into Practice*, 47(3), 220–228. <https://doi.org/10.1080/00405840802153916>
- Robin, B. (2016). The power of digital storytelling to support teaching and learning. *Digital Education Review*, 30(30), 17–29. <https://doi.org/10.1344/der.2016.30.17-29>
- Robin, B. (2011). *The educational uses of digital storytelling*. In Proceedings for the Society for Information Technology & Teacher Education International Conference (pp. 1264–1271). Association for the Advancement of Computing in Education (AACE).
- Robin, B. R. (2008). Digital storytelling: A powerful technology tool for the 21st century classroom. *Theory into Practice*, 47(3), 220–228. <https://doi.org/10.1080/00405840802153916>
- Robin, B. R., & McNeil, S. G. (2012). What educators should know about teaching digital storytelling. *Digital Education Review*, 22(1), 37–51. <https://doi.org/10.1344/der.2012.22.37-51>
- Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1), 95–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Rojon, C., & Saunders, M. N. K. (2012). Formulating a convincing rationale for a research study. *Coaching: An International Journal of Theory, Research and Practice*, 5(1), 55–61. <https://doi.org/10.1080/17521882.2011.648335>
- Safaricom PLC. (2017). *Leaving no one behind*. https://www.safaricom.co.ke/sustainabilityreport_2017/wp-content/uploads/2017/10/Safaricom_2017.pdf
- Safaricom PLC. (2018). *#Jitambulisha leo on 456*. - YouTube. https://www.youtube.com/watch?v=CDM1_yaKHNs
- Saracco, D. (2008). Why and How Assessment of Organization Culture Shapes Security Strategies. In H.F. Tipton., & M. Krause(Ed.), *Information Security Management Handbook* (Vol. 2, pp. 129–154). Auerbach Publications. <https://doi.org/10.1201/9781420067101>
- Saunders, M. N. K., & Rojon, C. (2014). There’s no madness in my method: Explaining how your coaching research findings are built on firm foundations. *Coaching*, 7(1), 74–83. <https://doi.org/10.1080/17521882.2014.889185>
- Serianu. (2017a). *Africa Cybersecurity Report*. <http://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>
- Serianu. (2017b). *Demystifying Africa’s Cyber Security Poverty Line*. <https://doi.org/https://serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>
- Serianu. (2018). *Cyber Security Skills Gap*. Africa Cyber Security Report - Kenya. <https://serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
- Silver, L., & Johnson, C. (2018). *Basic mobile phones more common than smartphones in sub-Saharan Africa* Pew Research Center. Pew Research Center. <https://www.pewresearch.org/global/2018/10/09/majorities-in-sub-saharan-africa-own-mobile-phones-but-smartphone-adoption-is-modest/>
- Skinner, T., Taylor, J., Dale, J., & McAlaney, D. J. (2018, April 4-6). *The development of intervention E-learning materials and implementation techniques for cyber-security behaviour change*. In Convention of the Study of Artificial Intelligence and Simulation of Behaviour (AISB), Liverpool, UK.
- Standard, I. (2011). *ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management*. <https://www.iso.org/standard/56742.html>
- Statista. (2017). *Kenya mobile cellular subscriptions 2000-2017* Statistic.


- <https://www.statista.com/statistics/498385/number-of-mobile-cellular-subscriptions-in-kenya/>
- Statista. (2019). *Number of mobile phone users worldwide*. The Statistics Portal. <https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>
- Stenitzer, G. (2015). Why Kenya leads the world in mobile money. *Global Telecoms Business*, 140, 22–23.
- Syssec. (2013). *The Red Book. A Roadmap for System Security Research (Resumé)*. <https://doi.org/10.13140/RG.2.1.1400.2000>.
- Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A risk assessment method for smartphones. In: Gritzalis D., Furnell S., Theoharidou M. (eds) *Information Security and Privacy Research. SEC 2012. IFIP Advances in Information and Communication Technology*, (Vol 376.,pp.443-456) Springer https://doi.org/10.1007/978-3-642-30436-1_36
- Thomas, D. R., Beresford, A. R., & Rice, A. (2015). *Security metrics for the android ecosystem*. Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices,(pp. 87–98). Association for Computing Machinery <https://doi.org/10.1145/2808117.2808118>
- Tschakert, K. F., & Ngamsuriyaraj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6), e02010. <https://doi.org/10.1016/j.heliyon.2019.e02010>
- van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human Computer Studies*, 123, 29–39. <https://doi.org/10.1016/j.ijhcs.2018.11.003>
- Venkatesh, Morris, Davis, & Davis. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3),425–478. <https://doi.org/10.2307/30036540>
- Venkatesh, Thong, & Xu. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly*, 36(1), 157–178. <https://doi.org/10.2307/41410412>
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, 17(5), 328–376. <https://doi.org/10.17705/1jais.00428>
- Wang, W., & Liu, Y. J. (2009). Attitude, behavioral intention and usage: An empirical study of Taiwan Railway’s internet ticketing system. *Taiwan: National Taiwan Ocean University*, 72. <http://www.swdsi.org/swdsi2009/papers/9c04.pdf>
- Weber, E. U., Blais, A. R., & Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, 15(4), 263–269. <https://doi.org/10.1002/bdm.414>
- Weick, K. E. (1995). What Theory is Not, Theorizing Is. *Administrative Science Quarterly*, 40(3), 385. <https://doi.org/10.2307/2393789>
- Westcott, R., Ronan, K., Bambrick, H., & Taylor, M. (2017). Expanding protection motivation theory: Investigating an application to animal owners and emergency responders in bushfire emergencies. *BMC Psychology*, 5(1), 1–14. <https://doi.org/10.1186/s40359-017-0182-3>
- Wetzel, A. P. (2010). Internet, mail, and mixed-mode surveys: The tailored design method *Journal of Continuing Education in the Health Professions*, 30(3), 206. <https://doi.org/10.1002/chp.20083>
- Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816. <https://doi.org/10.1016/j.chb.2008.04.005>

Zhang-Kennedy, L., Baig, K., & Chiasson, S. (2017, July 13-17). *Engaging children about online privacy through storytelling in an interactive comic*. [conference session] Electronic Visualisation and the Arts (EVA 2017), London. <https://doi.org/10.14236/ewic/HCI2017.45>

APPENDIX 1: RESEARCH PERMITS


APPENDIX 1A: NACOSTI LICENSE


REPUBLIC OF KENYA


**NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY & INNOVATION**

Ref No: **228563** Date of Issue: **19/September/2019**


RESEARCH LICENSE



This is to Certify that Ms.. Lynet Kosgey of Kenya Methodist University, has been licensed to conduct research in Nairobi, Uasin-Gishu on the topic: SMARTPHONE SECURITY AWARENESS MODEL AMONG KENYAN USERS_ BEHAVIORAL INTENTION for the period ending : 19/September/2020.

License No: **NACOSTI/P/19/1538**

228563
Applicant Identification Number


Director General
**NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY &
INNOVATION**

Verification QR Code



**NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.**

APPENDIX 1B: KeMU Introduction Letter



Kenya Methodist University

P. O. Box 267 - 60200, Meru, Kenya, Tel: (+254-020) 2118423-7, 064-30301/31229 Email: info@kemu.ac.ke, Website: www.kemu.ac.ke

September 9, 2019.

TO WHOM IT MAY CONCERN

RE: KOSGEY JESANG LYNET CIS-3-2235-1/2016

This is to confirm that the above named is a student in the Department of Computer Science, in this university, pursuing a Master of Science in Computer Information System.

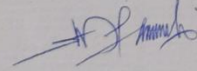
As a requirement, the student is expected to undertake an independent **primary research** in their area of specialization.

The purpose of this letter is therefore; to introduce the student to you and request you to allow him undertake the research in your organization.

The student has been advised to ensure that all data and information from the organization is treated with utmost confidentiality and only used for academic purposes unless otherwise stated.

Any assistance accorded to her will be highly appreciated.

Yours faithfully,


Dr. Peter Kihara, PhD
Registrar -Academic Affairs



Nairobi Campus: Koinange Street, P.O. Box 45240-00100 Nairobi - Tel: +254-20-2118443/2248172/2247987/0725-751878 • Email: nairobicampus@kemu.ac.ke
Nakuru Campus: Mache Plaza, 4th Floor. P.O. Box 3654-20100, Nakuru, Tel +254-51-2214456 • Email: nakurucampus@kemu.ac.ke
Mombasa Campus: Former Oshwal Academy, P.O. Box 89983, Mombasa. Tel: +254 - 041-2495945 / 8 • Email: mombasacampus@kemu.ac.ke

The Future is Here!

APPENDIX 2: QUESTIONNAIRE

APPENDIX 2A: PHASE 1

Research Questionnaire

I appreciate your interest in participating in a study regarding smartphone usage. Simply answer the questions and click the next arrow button in the lower portion of your screen.

A few things to note before we begin:

Your Answers are completely Confidential and hence it will be recorded anonymously This Survey is for academic purposes only

Contact me if you have any questions (infoseclyn@gmail.com)

Section I: Background information

1. Please choose one category that best describes your current profession. Mark only one oval.
 - Working or Self-Employed Student
 - Retired
 - Unemployed
2. Do you have a smartphone? * Mark only one oval.
 - Yes
 - No
3. What level of IT proficiency do you categorize yourself at? Mark only one oval.
 - Good
 - Moderate
 - Excellent
 - Do not have IT knowledge
4. What is the operating System on your phone? Mark only one oval.
 - Android by Google IOS by Apple BlackBerry Windows Phone
 - I am not Aware
5. Which country do you live in?
6. What kind of setting do you reside in? Mark only one oval.
 - Rural Urban
7. Is the phone that you have controlled/monitored by your employer? Mark only one oval.
 - Yes
 - No

Section II- Objective III-Security Countermeasure Awareness

8. Where do you get the applications to install on your phone?

- Check all that apply.
- Via official store i.e Play Store and Apple Store only I get it from friends
- Websites
- Not Aware
- Other:

9. What are the factors you consider while installing an application (tick all that applies)?

- Check all that apply.
- Price
- User Review
- Familiarity with the brand
- Friends Recommendation
- End User License agreement and terms of service Popularity
- Screenshots
- Search Ranking
- Application Privacy Policy
- Application Permissions
- Other:

10. Do you pay attention to security messages that appear on your phone during installation?

Mark only one oval.

- Yes, for every application
- Only, for some application
- No, I do not really bother

11. Do you pay attention to security messages that come to your phone informing you of a promotion or a discount?

Mark only one oval.

- Yes, for every message
- Only, for some message
- No, I do not really bother

12. Do you verify links and messages shared before opening? Mark only one oval.

- Yes
- No

13. Do you keep your pin and password confidential? Mark only one oval.

- Yes
- No

Section III: Objective I-User Threat Awareness

14. Please answer the following statements to the best of your knowledge Mark only one oval per row.

Yes, No, I am not Sure

- 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?
- Do you sometimes forget to disable locational service GPS, on your phone after use?
- Do you know/have stored your smartphones IMEI (International Mobile Equipment Identity) number?
- Do you erase your smartphone before you give it to the next user?
- Do you sometimes connect to public WIFI when performing transactions?
- Have you set a pin, password or any physical control on your phone?
- Do you update your phone and mobile applications regularly?
- Do you click on any link or scan QR code shared?

15. What type of security and/or software do you have on your Smartphone? Check all that apply.

- Antivirus or Anti-Malware
- Locking with Password, Pin or Fingerprint Encrypting phone Data
- Back Up phone Data
- Phone Update
- Avoiding Public WiFi
- Being Aware of Phone Scam or suspicious contents Disabling Location Services
- Installing only trusted applications
- Other:

Section IV: Objective II User Risk Perception

16. Do you consider smartphone antivirus important? Mark only one oval.

- Yes
- No

17. On what device do you install antivirus or firewall? Check all that apply.

- Smartphone/Tablet
- PC/Laptop/Notebook Other:

18. Please answer the following statements to the best of your knowledge Mark only one oval per row.

- Are you aware that some application updates improve your phone security?

Yes, No, I am not Sure

- Are you aware that some links shared or QR code to scan are not legit?
- Are you aware that application may contain Spyware that can access private information on your smart phone?
- Some banking application pose as legit but instead steal your banking information, Are you aware of this?
- Smartphone can be transferred to another user without properly removing sensitive information. Are you aware of this?
- Are you aware that smartphone can connect to open/insecure public Wi-Fi hotspots hence exposing you to personal and financial data?

Section IV: Objective II User Risk Perception

19. Please answer the following statements to the best of your knowledge Mark only one oval per row.

Very great extent

Small extent

Very small extent

Do not know

- I am concerned that some applications can access private data on my Smartphone such as pictures, contacts, location, device information and others?
- I am concerned that Spyware can access my information without consent?
- I am concerned that my banking details can be stolen by malicious application?
- I am concerned that some sensitive data can be transferred from my smartphone to the next user?
- I am concerned that public Wi-Fi can expose my personal or financial data?
- I am concerned towards not creating a pin or password on my phone?
- I am concerned with the suspicious link or QR codes shared with me?

20. Does your current awareness of and concern about mobile security and Privacy, those described in the above questions impact your decision making in installing mobile protection on your phone?

Mark only one oval.

- Yes
- No

21. Kindly tell us more on how it impacts your decision

22. Do you think your level of exposure has influence the decisions you make, to protect your data on your smartphone?

Mark only one oval.

- No
- Maybe
- Yes

Section V: Demographics

23. What is your gender? Mark only one oval.

- Male
- Female
- Prefer not to answer

24. What is your age?

Mark only one oval.

- Less than 20 years
- 20-30 years
- 30-40 years
- 40-50 years
- Above 50 years
- Prefer not to answer

25. Please add any comment that you have in relation to the survey above

APPENDIX 2B: PHASE 2

Research on the use of Public WiFi

This questionnaire is part of research that seeks to investigate the effectiveness of digital storytelling on information security awareness, with a focus on use and exposure to public WiFi.

The questionnaire will require at most 10 minutes to complete.

Complete this questionnaire AFTER watching the video whose link you received with the questionnaire.

Your response is completely confidential and hence it will be recorded anonymously. This survey is for academic purposes only.

Researchers

- Lynet Kosgey (Postgraduate Researcher)
- Mwaniki Nyaga (Contributing Researcher)
- Dr. Chao Mbogho (Postgraduate Supervisor)
- David Munene (Postgraduate Supervisor)

The form will go offline on Saturday, Aug 15th, at midnight.

In case of any questions or concerns please contact the researchers at infoseclyn@gmail.com

Background Information

1. Which country do you reside in?

Mark only one oval.

Kenya Outside Kenya

If in Kenya, select which of these parts you currently reside in.

Mark only one oval.

Nairobi City Mombasa City Kisumu City Other:

2. What kind of setting best describes your residency? Mark only one oval.

Rural Urban

3. Please select your age group Mark only one oval.

Below 20 years old 20 - 30 years old

30 - 40 years old

40 -50 years old

Above 50 years old

Prefer not to answer

4. Please choose one category that best describes your current profession. Mark only one oval.

Working or Self-Employed Student

Retired

Unemployed

5. What is your IT proficiency level? Mark only one oval.

Good

Moderate

Excellent

Don't have IT knowledge

6. Have you previously viewed an informational video or advertisement that seeks to spread awareness on any of the following information security issues related to the use of MOBILE DEVICES?

Mark only one oval per row. Yes No

Use of public WiFi

Use of antivirus software

Use of passwords (pin, fingerprint, voice)

Encrypting data

Phone software updates

Awareness of scams and untrusted content

Disabling location services

Installing trusted applications

Video Evaluation

7. After watching the video, please rate the following aspects

Mark only one oval per row.

The video was fun

The video was easy to understand

I am willing to share the video

8. While watching the video how well did you understand the following aspects:

Mark only one oval per row. Not at all Slightly Moderately Very Extremely

The chances of becoming a victim of a public WiFi attack

The risks involved with public WiFi & their consequences

Users' concern with using public WiFi

How you can prevent attacks from public WiFi

When you can prevent attacks from public WiFi

The benefits of carrying out secure behaviour

9. AFTER WATCHING THE VIDEO what is the likelihood of you embracing the following secure practices?

Mark only one oval per row. Not Likely, Slightly Likely, Likely, Fairly Likely, Very Likely

Avoiding to check sensitive data while on public WiFi

Using a VPN or HTTPS to access sensitive data while on public WiFi

Asking an employee for their actual public WiFi credentials

Not leaving/turning on auto- connect while on public WiFi

Not leaving WiFi turned on after using public WiFi

Additional Information

10. What did you like about the video?

11. What did you dislike about the video