UNIVERSITY OF KWAZULU-NATAL

Information Security Education, Training, and Awareness within the Mobile Financial Services Sector

Nicholas Washington Omollo
Student No. 212559707

A thesis submitted in fulfilment of the requirements for the degree
of
Doctor of Philosophy

School of Management, IT, and Governance
College of Law and Management Studies

Supervisor: Professor Manoj Maharaj

2025

Candidate Declaration

I, **Nicholas Washington Omollo**, declare that:

i. The research reported in this thesis, except where otherwise indicated, is my original research.

ii. This thesis has not been submitted for any degree or examination at any other university.

iii. This thesis does not contain other persons' data, pictures, graphs, or other information, unless specifically acknowledged as being sourced from other persons.

iv. The thesis does not contain other persons' writing unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

   a. their words have been re-written, but the general information attributed to them has been referenced;

   b. where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. Where I have reproduced a publication of which I am an author, co-author or editor, I have indicated in detail which part of the publication was actually written by myself alone and have fully referenced such publications.

vi. This thesis does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

NICHOLAS WASHINGTON OMOLLO

Dedication

To the loving memory of my dear mother and father,
whose values, sacrifices, and dreams continue to guide and inspire me.

To my wife, whose unwavering support, patience, and belief in me made this journey possible.

To my son and daughter,
may this work show you the value of perseverance, purpose, and education.

With deepest love and gratitude.

Acknowledgements

The author expresses gratitude to God for the support provided during the study. Additionally, the author acknowledges Professor Manoj Maharaj, the supervisor, for the guidance and motivation offered throughout the study. Despite challenging circumstances such as sickness and setbacks, the professor's counsel and support have been a source of encouragement to the author.

Furthermore, the author extends thanks to the survey respondents for accepting to take part in this study. The author would also like to appreciate all members of his family for their encouragement, love, and support during this study. The author acknowledges that the family's unwavering support and encouragement have been instrumental in achieving the study's goal.

Abstract and Key Words

Previous research has underscored the critical role of integrating technology, processes, and human factors in ensuring the resilience and security of Information Technology (IT) systems. Often, failures in IT systems within organizations stem not from technological weaknesses, but from insufficient user awareness regarding security protocols. This study delves into the significance of Information Security Awareness (ISA) in fostering secure behaviours among users of Mobile Financial Services (MFS) in Kenya. Through an examination of factors contributing to effective cybersecurity awareness initiatives, this research offers valuable insights for organizations evaluating the role of ISA in enhancing the cybersecurity practices of MFS users.

Adopting an interdisciplinary approach that merges insights from financial services and information systems disciplines, this study draws on data collected from five counties in Kenya using questionnaires. The study encompasses 1159 MFS users and 23 professionals engaged in providing financial services through mobile channels. Results reveal that 52% of respondents experienced financial losses due to fraudulent mobile money transactions, while a significant 69% had never participated in any awareness sessions on mobile security. These findings underscore the pressing need for comprehensive training programs to instil secure behaviours among MFS users, particularly in light of the escalating adoption of MFS.

To establish a robust framework for cybersecurity awareness tailored to MFS, the study adopts the NIST and MediaPro Adaptive awareness frameworks. Through thorough analysis, the research proposes the Adaptive Governance Awareness Model (AGAM). This model offers strategic guidelines for planning, evaluating, and implementing cybersecurity awareness initiatives targeting MFS users, thereby enhancing overall cybersecurity resilience within the MFS ecosystem.

Key Words: Awareness; Cybersecurity; Information Privacy; People Errors; Mobile Money.

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

AGAM	Adaptive Governance Awareness Model
ATM	Automatic Teller Machine
CAK	Communications Authority of Kenya
CBK	Central Bank of Kenya
CBT	Computer-Based Training
CCPA	California Consumer Privacy Act
CIA	Confidentiality, Integrity, and Availability
DFS	Digital Financial Service
DID	Defence in Depth
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRP	Data Recovery Plan
ENISA	European Union Agency for Network and Information Security
EU	European Union
FY	Financial Year
GDPR	Global Data Protection Regulation
GLBA	Gramm-Leach Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
ICT	Information Communication Technology
ID	Instructional Design
IPS	Intrusion Prevention System
IS	Information Systems

IT	Information Technology
KYC	Know Your Customer
KZN	KwaZulu-Natal
LSA	Lead Supervisory Authority
MFS	Mobile Financial Services
MM	Mobile Money
MNO	Mobile Network Operator
MSCTM	Mobile Secure Content and Threat Management
MSISDN	Mobile Station International Subscriber Directory Number
NFC	Near-Field Communications
OS	Operating System
OWASP	Open Web Application Security Project
PII	Personal Identifiable Information
PIN	Personal Identification Number
QR	Quick Response
RSA	Republic of South Africa
SA	South Africa
SMS	Short Message Service
SSL	Security Socket Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TPB	Theory of Planned behaviour
UK	United Kingdom
UKZN	University of KwaZulu-Natal

Chapter 1: Introduction and General Overview of the Study

You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable.

Daryl White, DOI CIO

1.1. INTRODUCTION

Information is a vital and most valuable asset to any organisation and should be well protected (Bhardwaj & Kaushik, 2022; Farooq et al., 2022). The main information characteristics of Confidentiality, Integrity, and Availability, or the CIA-triad, provide value. Even the most successful organisation may be brought down if there is a compromise of its information confidentiality, integrity, and availability (ISO/IEC 27002, 2022). Therefore, organisations must protect their information resources to avoid rendering such information meaningless.

In recognition of the importance of protecting information in Kenya, Data Protection Act (DPA) was enacted on November 25, 2019 (Government of Kenya, 2019). The enactment of this Act upholds Article 31 of The Constitution of Kenya (2010), which recognizes privacy as a basic human right. Under the framework of the Data Protection Act (DPA), the processing of personal data by organizations is regulated. Notably, entities offering Mobile Financial Services (MFS) fall within the scope of this legislation. Given that MFS operations involve the handling of sensitive customer information, stringent measures are imperative to ensure the protection of personal data and the preservation of individuals' privacy rights as stipulated by the DPA. Moreover, these organizations must reassure regulatory bodies and customers alike of the adequacy of their information protection measures.

Mobile Financial Service providers are exploiting the business opportunities brought by mobile communications technologies. Mobile Financial Services (MFS) offer customers anytime, anywhere financial service convenience, thereby accelerating the adoption of these services. MFS has placed an additional obligation on the users and service providers to exercise an intensified level of control, which requires specialised training, education, and awareness. The question Whitney (2021) poses is why there is a lack of knowledge among end-users regarding cyberattacks, cybersecurity, and the risks they expose organisations to. User awareness aims to enhance users' security behaviour, constituting a vital component of information security.

Information security is defined as protecting an organisation's information from various threats that could disrupt business continuity, increase business risks, and lower investment returns, thus inhibiting growth (Whitman & Mattord, 2021). Information security as a discipline involves protecting an organisation's information through implementing security controls. To safeguard an organisation's information, a comprehensive array of measures must be employed, including procedural protocols, well-designed organisational structures, thoughtfully crafted policies, and robust hardware and software. These combined efforts serve to mitigate risks and reduce the vulnerability of sensitive information to an acceptable level (ISO/IEC 27002, 2022). Therefore, access control is an important security mechanism that requires adequate consideration (Alsmadi et al., 2018).

The risk level associated with information protection can be considerably reduced by implementing various physical and technical controls. Such controls can be chosen from information security standards accepted nationally and internationally. Various information security standards exist from which organisations can select, including COBIT 5 and ISO 27002. The operating framework of an organisation's technical and physical controls is still greatly influenced and directly linked to people – referred to as the "human factor." Good security is achieved through a combination of technical measures, a solid understanding of information security issues by users, and the security practices to protect themselves (Talib et al., 2010). Technical solid protective measures are useless if an attacker can still successfully influence users of any system (Grassegger & Nedbal, 2021). Studies show that the "human factor" relating to poor planning by solution providers, ignorance, and inability to pay attention to detail on the part of users of information systems contribute to the rise in security breaches by accidental or unintentional insiders (Hadlington, 2021). Consequently, addressing the "human factor" must be a focal point in an organization's information security planning, recognizing that effective security measures necessitate not only technical solutions but also comprehensive strategies that account for human behaviour and engagement.

Preserving the CIA of information assets against risks and attacks in this digital age is challenging for organisations (Khando et al., 2021). Hence, organisations across the globe are increasingly allocating resources to adopt advanced technology aimed at safeguarding their valuable information assets. Nonetheless, despite substantial investments in information security solutions, numerous instances of failure have been observed. This can be attributed to the fact that certain technical measures employed are either incompatible with existing systems

or prove inadequate in effectively countering potential threats. A significant amount of money spent on protecting information systems focuses on technical defences against external threats, which is often exaggerated, whereas 60% to 85% of all information security incidences result from a lack of knowledge or understanding among users (McIlwraith, 2021). Many information security incidents witnessed in organisations result from the exploitation of human elements either indirectly or directly (Khando et al., 2021). Information may lose its confidentiality, integrity, and availability due to users' unintentional or accidental influence on the operational controls implemented by an organisation (Kritzinger & Smith, 2008). For instance, an operational control could require a user to log off from their workstation and then lock the office door before leaving. Ignoring this procedure would render the technical and physical control useless. "Insider threats" are increasingly considered a significant challenge to cybersecurity, but they can be detected and apprehended by implementing appropriate mechanisms (Hadlington, 2021).

Many end-users consider information security as the responsibility of the IT department, while others view it as a secondary priority that comes after their work. As a result, educating users about information security is essential, providing them with adequate and appropriate knowledge. Information security awareness is critical to protect against undesirable user information security behaviours (Khando et al., 2021). Therefore, every user becomes the most vital linkage regarding information protection if given the relevant awareness training on cybersecurity. Thus, cybersecurity awareness is consistent with the Defence in Depth (DID) approach, which is essential in realising Information Assurance (IA) in a connected environment (Yeboah, 2013). Achieving Information Assurance requires that the organisation balances focus on three primary elements: Technology, Operations, and People, which are essential principles of the DID strategy (Yeboah, 2013). Therefore, by educating end-users, the organisation may enlighten users about the DID the organisation has employed (Downer & Bhattacharya, 2022). An effective user protection awareness campaign will significantly improve an organisation's IA posture (Kiruthika & Chakravarthy, 2019).

1.2. BACKGROUND AND CONTEXT

There has been constant innovation in the Financial Service Sector by providing technology-enabled services. The latest is the provision of mobile banking services. In the year 2007, Safaricom, the largest mobile network operator in Kenya, introduced M-PESA, which has since

become the flagship example of mobile money services (Sridhar, 2022). A recent report by Nelito (2021) examines the landscape of mobile money service providers in Kenya, highlighting four prominent players, namely Safaricom M-PESA, Airtel Money, Orange T-Cash, and Essar yuCash. Nevertheless, the market is overwhelmingly dominated by Safaricom's product, M-PESA (CAK, 2021). In the report, just four years after M-PESA's launch, it had 1072 branches across Kenya, but this has grown to 46 000 agent outlets providing mobile money services. The Communications Authority of Kenya, in its Q1 of 2021–2022 Financial Year (FY), published the Sector Statistics report revealing that Safaricom commands a market share of 98.5%, Airtel Money 0.8%, and T-Cash commands 0.7%. A report by Vodafone (2022) indicates that M-PESA, with over 604,000 agents that operate across Kenya, Ghana, Mozambique, Democratic Republic of Congo (DRC), Tanzania, Egypt, and Lesotho, is Africa's leading mobile money service. The annual report of the Central Bank of Kenya (2021) indicates that Kenya hit a historic high in mobile money transactions after users transacted Kshs 6.24 trillion (US $52.1 billion) using their mobile phones from January to November 2021. This figure of Kshs 6.24 trillion was Kshs 9.2 billion more than the value transacted between January to December 2020.

Based on the data presented in the Communications Authority of Kenya Sector-Statistics-Report-Q1-2021-2022 FY (2021: 11), mobile money subscriptions in Kenya amounted to 34.59 million during the specified quarter. This figure indicates a notable growth of 8.8% when compared to the 31.8 million subscribers recorded in Q1 of the previous financial year. During that period, Person-to-Person transactions valued at Kshs 1.082 trillion ($9.092 billion) were transacted compared with Kshs 896.5 billion in the same period, the previous FY, a 20.7% increase. In that same period, customer-to-business money transfers (paying for goods and services) valued at Kshs 1.196 trillion were transacted compared with Kshs 735.9 billion transacted the previous year, representing a 62.6% increase. This rapid uptake of mobile money shows the continued demand for mobile financial services.

Table 1.1 Kenya's Mobile Money Service

Mobile Money Brand/Indicator	July-Sep 2021	Apr-Jun 2021	Quarterly Variation (%)
No. of Registered Agents	289,095	283,357	2.0
Value of C2B Transfers in KES	1,196,391,334,211	988,018,815,400	21.1
Value of B2C Transfers in KES	817,677,356,335	721,923,115,562	13.3
Value of B2B Transfers in KES	1,960,759,312,250	1,708,523,490,893	14.8
Value of G2C Transfers in KES	1,885,367,083	2,671,076,965	-29.4
Value of C2G Transfers KES	12,331,336,677	11,576,180,527	6.5
Volume of P2P Transfers	912,039,926	838,263,623	8.8
Value of P2P Transfers in KES	1,081,900,345,466	1,010,533,046,147	7.1
Total Value of Deposits in KES	**1,181,270,848,413**	**1,018,040,156,765**	**16.0**

Key: C2B- Customer-to-Business, B2C- Business-to-Customer, B2B- Business-to-Business, G2C- Government-to-Customer, C2G- Customer-to-Government, P2P- Person-to-Person.

Source: CAK (2021)

A report by the Kenya National Bureau of Statistics (Oluwole, 2022) indicates a 63% surge in mobile money transactions in 2021 compared with the year 2020, with total transaction value rising from $78.3 billion in the year 2020 to $127.5 billion in 2021.

Globally, there has been tremendous growth in the adoption of mobile money services. A state of the industry report by GSMA (2021), the industry body for the Global System of Mobile Communications, shows that international remittances processed through mobile phones stood at $767 billion, an increase of 65% compared with transactions in 2020. The report also showed that there were 1.2 billion registered mobile money accounts globally, with over $2 billion being transacted daily by the mobile money industry. Similarly, Boston Consulting Group (Sénant et al., 2020), an American research firm, produced a report showing that Kenya and Ghana are still dominating the global mobile money market, coming at positions two and three, respectively, after China which recorded the highest mobile payment usage.

Traditional banking, in most cases, is out of range for the poor and unbanked population due to certain limitations, including infrastructure, time, and other resources. Mobile banking then provides a possible answer to these limitations and offers flexible and convenient banking to the poor, bringing them to mainstream banking. Mobile banking brings cost and convenience

benefits since these services match the customer's location (Windari et al., 2022). Over the years, technology has developed, and many security methods are available in the market to enable banks to provide mobile banking solutions that guarantee prompt delivery of banking services to clients enabling seamless remote transactions. The introduction of mobile banking solutions has brought flexibility to financial transactions while simultaneously increasing the risk of financial fraud (Tiwari, 2019). Al-Delayel (2022) says the mobile banking applications possess access to confidential information for every customer, consequently creating a potential avenue for attack for the bank and the client. Tiwari (2019) notes that, while many people feel more comfortable carrying out transactions over their mobile handsets, they need to be made aware of the threats that mobile banking technology poses. Awareness of users is an important measure that helps reduce the risk of disclosing sensitive information to attackers (Iser & Brandtweiner, 2022).

Most data breaches in organisations are caused by human errors rather than technology failure (Quagliata, 2012). For this reason, Hughes-Lartey et al. (2021) suggest that the strength of any sound information security system is not just in the technology but rather in the hands of the users. Most data breaches faced by organisations are, to some extent, linked to the manipulation of human resources in terms of user behaviour or the errors committed by the users (Klahr, et al., 2017; Spremić & Šimunic, 2018). To deal with this problem, information security professionals have consistently emphasised the importance of having a robust SETA programme in every organisation. Razack (2022) adds that having an awareness programme alone is insufficient. Quagliata (2012) raises the alarm that although the necessity for cybersecurity awareness training has been recognized, study has not been undertaken to establish the most effective components of that SETA programme. While cybersecurity training is commonplace in many organisations, the effectiveness of these training offerings is questioned since many reports of increasing successful cyber-attacks are being witnessed (Chowdhury et al., 2022). Razack (2022) posits that users need to appreciate the ethical and legal implications of failing to conform with cybersecurity guidelines and best practices. He adds that a SETA programme is more effective if it explains why the programme is essential (user attitudes) instead of just outlining what is expected (knowledge to be acquired).

This study established the most effective cybersecurity awareness training programme components for users of mobile financial services. The researcher undertook the development

of a foundational body of knowledge concerning cybersecurity awareness training for end-users engaged in mobile financial services. This initiative aims to enhance the overall security

1.3. STUDY CONSTRUCTS

This study utilizes constructs from two theoretical frameworks: the NIST Cybersecurity Framework and the MediaPro Adaptive Awareness Framework. No single model would have sufficiently covered the study; hence, a hybrid model combining constructs from both frameworks was constructed, resulting in the proposed model.

1.4. STATEMENT OF THE PROBLEM

Cybercrime, real-life assaults, and mobile fraud occurring worldwide have led individuals to recognize their vulnerability. This realisation has prompted a shift in their perspective on information security. Organisations can no longer relegate cybersecurity awareness training to the side-lines. The era when only a select few information security experts, such as Cybersecurity Specialists and System Administrators, would be educated and trained on information security is over (McIlwraith, 2021; Alshaikh & Adamson, 2021). Information security is now everyone's responsibility. Razack (2022) argues that management should serve as role models, fostering a culture of cybersecurity in which it is viewed as everyone's duty, not solely the duty of the cybersecurity team.

A study conducted among Kenyan financial institutions revealed significant losses due to fraud (Fakiya, 2023). A credit referencing agency, TransUnion Africa, reported that Kenyan banks lose over Kshs 13 billion ($121.49 million) annually through loan stacking and identity theft (The East African, 2021). A FinAccess survey report indicates that half of mobile money users fall victim to fraudsters (FSD, 2021). The report disclosed that 47.4% of mobile money users in Kenya have reportedly lost money, a substantial increase from the 8.4% who reported losses in 2019. This surge is attributed to the growing preference for mobile money services amid COVID-19, as the use of physical cash was discouraged to help reduce viral transmission. The report further revealed that seven out of 10 individuals mistakenly sent money to the wrong recipients, who withdrew the funds and refused to refund them. Additionally, the report showed that Kenyans lost money through hoax SMS messages, phone calls, fraud, and cybercrime affecting both bank and mobile bank accounts. The report indicated that fraud was the most significant risk for bank account users, with 34.5% of respondents stating that the

crime occurred internally through bank employees, while 25.9% of the fraud took place via phone.

A UK Finance half-year Fraud Update Report (2021) demonstrated that criminals stole £753.9 million ($867.8 million) through fraud, representing a 30% increase compared to H1 of 2020. The report revealed that fraudsters employed tactics such as text messages, emails, fraudulent phone calls, social media posts, and fake websites to deceive individuals into providing their passwords and personal information. A global banking fraud survey report by KPMG International indicated that the most prevalent types of global fraud between 2015 and 2018 included cyber-attacks, identity theft, account takeovers, push payment swindles, and card-not-present swindles (KPMG, 2019). The report showed that less than 25% of fraud losses could be recovered and argued that customers play a crucial role in detecting and preventing fraudulent activity in their bank accounts, emphasising the importance of educating customers about swindles and fraud.

The utilisation of portable devices for financial transactions has shown a notable rise in profitability for criminals who target these platforms (Ayyash, 2022). Over a period of 17 months ending in March 2021, savings and credit cooperative societies in Kenya lost Kshs 106 million ($884 000) due to cyber theft, driven by the increased use of digital channels for financial transactions (Wanaswa, 2022). Although the banking application may be legitimate, users are not guaranteed secure transactions (Ayyash, 2022). Kenyan financial institutions must take more significant measures to curb the rising number of fraud cases.

Technological advancements introduce new methods for fraudsters to deceive or steal from unsuspecting customers (Otieno, 2021). Financial service providers must always stay one step ahead of these criminals to protect funds. Cranfield et al. (2020) observed that education and awareness training for end-users is essential in addressing mobile device security concerns, which concurs with Union Bank (2022), suggesting that the initial step to protect against fraud is to equip oneself with relevant information.

While the critical cost of mobile financial services is security, the most significant benefit is convenience (He et al., 2015). Mobile financial service providers and users have not been seriously tackling this security issue surrounding mobile financial services. Dash and Ansari (2022) argue that cybersecurity awareness training serves as an effective intervention. Based on the researcher's survey of the mobile financial services industry, it has been observed that

there is currently a lack of a well-defined model for cybersecurity awareness training to effectively address and mitigate the cybersecurity challenges prevalent in the mobile financial services sector. The absence of such a model poses a considerable obstacle in ensuring the robust protection of sensitive financial data and safeguarding against potential cyber threats and vulnerabilities. This study sets out to fill the gap caused by the absence of the model.

This study investigates the extent to which users adopt secure behaviour while interacting with mobile financial services and the role awareness plays in improving secure mobile financial services behaviour. Furthermore, the study identifies the theoretical constructs for information security awareness among users of mobile financial services, based on the NIST Cybersecurity Framework and MediaPro Adaptive Awareness Framework.

1.5. RESEARCH OBJECTIVES

The primary objective of this study is to identify the constructs of Adaptive Governance and Awareness Model (AGAM) that can be used to improve cybersecurity awareness among users of mobile financial services. The primary objective of this model is to bring about positive changes in the behaviour of MFS end-users, thereby enhancing the overall cybersecurity posture of the MFS ecosystem. Furthermore, the study presents a comprehensive list of information security concepts and topics that are considered crucial for inclusion in cybersecurity awareness training programmes.

The secondary objectives of the research were to:

i. To assist and guide policy makers in creating policy frameworks that take into considerations an understanding of information security among users of mobile financial services.
ii. Investigate mobile banking in Kenya, including the legislative framework for mobile banking solutions.
iii. Evaluate the weighted importance of each identified construct that influences the information security behaviour of mobile financial services users.
iv. Examine the state of mobile security training and awareness among users of mobile financial services.

The study sought to comprehend the mobile banking industry processes, the users of mobile banking services, cybersecurity challenges within mobile financial services, and cybersecurity

training and awareness objectives and their integration within mobile banking. The study went on to propose a baseline cybersecurity governance and awareness model, drawing inspiration from the NIST Cybersecurity Framework and MediaPro Adaptive Awareness Framework. The integration of the NIST Cybersecurity and MediaPro Adaptive Awareness frameworks offers a comprehensive and effective approach to cybersecurity awareness and training for mobile financial services users. The structured risk management processes of NIST combined with the adaptive, behaviour-focused training of MediaPro ensure a resilient and aware user base, capable of mitigating cybersecurity threats effectively.

1.6. RESEARCH QUESTIONS

This research study aims to develop an awareness training model for improving information security behaviour of end-users of mobile financial services. The primary research question underpinning this study: How does awareness training influence secure behaviour among users of mobile financial services?

i. Which concepts and topics on cybersecurity should be included in the Training, Education, and Awareness programmes?
ii. What are the fundamental components of an information security education programme?
iii. How does level of education, age and place of residence influence cybersecurity behaviour of users of mobile financial services?
iv. Which constructs borrowed from NIST Cybersecurity and MediaPro Adaptive Awareness frameworks can be used to improve cybersecurity awareness among users of mobile financial services?

1.7. SIGNIFICANCE OF THE STUDY

The development of mobile banking has led to the availability of mobile applications for users everywhere and at any time. Consequently, traditional technological firewalls that banks implemented to reduce risks might need to be replaced with other security measures. Most users perceive their mobile devices merely as phones rather than minicomputers. Moreover, they regard their phones as protected devices (GTISC, 2022). This belief influences how people handle their phones, the messages they receive, and the applications they use. GTISC (2022) thus recommends increasing awareness of the security risks that phones pose to users.

Much as the benefits of awareness training is well researched, little study has been done on the role it plays within the mobile financial services. This study will contribute to the gap in this knowledge area. The study will assist policy makers by providing information on the role of awareness training in improving secure behaviour among users of MFS.

1.8. STRUCTURE OF THE STUDY

This study is structured into six chapters:

i. **Chapter One.** This chapter introduces the study, providing the background, objectives, and study design required to achieve the stated objectives.

ii. **Chapter Two.** The literature underpinning the study is presented in this chapter.

iii. **Chapter Three.** The theoretical frameworks that form the foundation of the research are introduced in this chapter.

iv. **Chapter Four.** The methodology adopted in the research is presented in this chapter.

v. **Chapter Five.** The analysis of the research findings and reflections from the questionnaires are presented in this chapter.

vi. **Chapter Six.** The final chapter presents the study's conclusion.

1.9. CHAPTER SUMMARY

Technological developments have made banking and fund transfers between parties easier and more convenient with the advent of mobile banking. Intruders, like in an organisation, can access virtually any location on the information superhighway. For fraudsters, they can empty one's bank account and leave no trace. They can hack an organisation's website, halt internet servers and email systems, and disrupt processes, causing loss of business and productivity, and ultimately embarrassing the company. Through proper security policy, security awareness training programmes, potential losses resulting from such vulnerabilities and threats can be reduced to acceptable levels since the key to information security is not products but people. Protecting the mobile financial services infrastructure and customers' funds should remain a priority, just as traditional banking systems aimed to provide. Users require cybersecurity awareness training to effectively acquire the requisite knowledge and competencies, thereby cultivating appropriate behaviours that foster the security of mobile financial services.

The present study has formulated a novel model that constitutes a valuable addition to the existing body of knowledge concerning cybersecurity awareness training targeted at end-users. This model is designed to facilitate a prompt transformation of knowledge, behaviour, and attitude among individuals operating within various national and international industry sectors. By so-doing, it aims to reinforce sound information security practices, effectively enhancing the overall security posture of organisations and individuals alike.

Chapter 2: Literature Review

Security is both a feeling and a reality. You can feel secure even though you're not, and you can be secure even though you don't feel it.

— Bruce Schneier

2.1. INTRODUCTION

Information systems encompass various interrelated subsystems, including data, software, processes, and people. This chapter will discuss these components, beginning with a description of the concept of an IT system, the growth and acceptance of Mobile Financial Services (MFS), security and privacy in MFS, security theatre and its impact on effective security, the cybersecurity learning continuum, and factors contributing to successful cybersecurity education training and awareness (SETA) initiatives. Finally, this chapter will examine the current state of these research areas, present trends in these fields, and identify any shortcomings or limitations in the existing literature.

2.2. THE CONCEPT OF AN INFORMATION TECHNOLOGY (IT) SYSTEM

An Information Technology (IT) System is an integrated component that collects, processes, and stores data, providing organisations with information and knowledge. Three fundamental components constitute an IT system: People, Technology, and Processes (Simon, 2021). These three components are depicted in Figure 2.1.

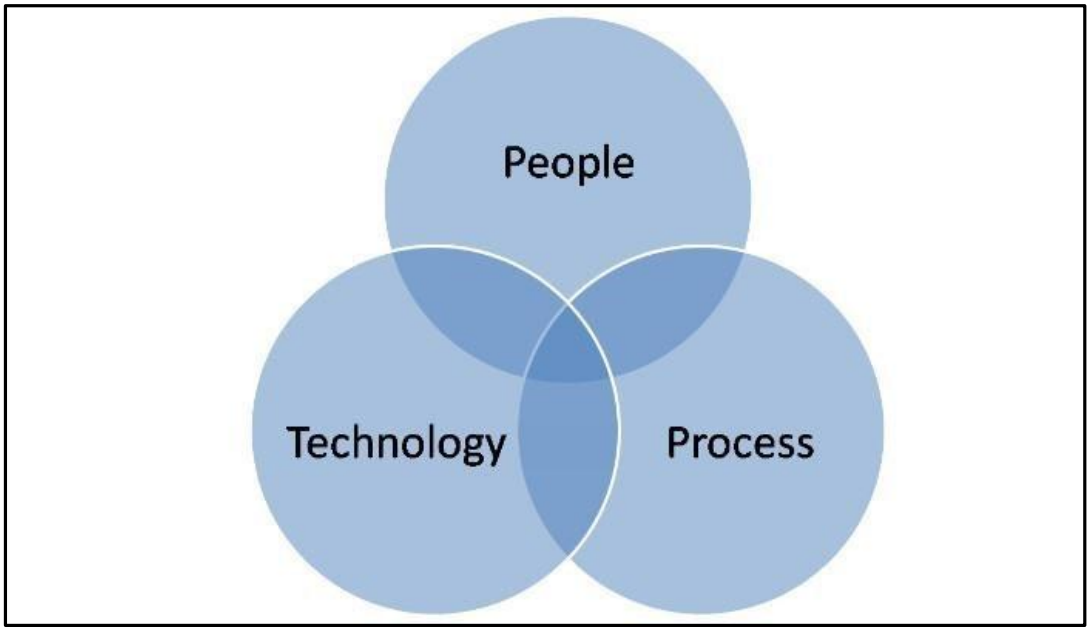


Figure 2.1 Components of an IT System

Source: Simon (2021)

These three components can be described as follows:

i. Technology: This refers to hardware and software. Hardware can be active and thus is configurable like switches and servers or passive, e.g., hubs. Software includes Operating systems and application systems.
ii. People: This encompasses a diverse range of stakeholders, including customers, employees, partners, former employees, competitors, suppliers, consultants, hackers, and other relevant entities.
iii. Processes: This refers to the interactions between people and processes data or information to produce outputs. Data can include financial, employee, customer, payroll, and medical records, among others.

A conceptual view of people reveals that it consists of individuals within the organisation (insiders) and those outside the organisation (outsiders). Therefore, it can be concluded that cyberattacks on an organisation can originate from both insiders and outsiders.

The overall objective of the information security programme is the protection of an organisation's information assets – Confidentiality, Integrity, and Authenticity (CIA) (Russell, 2002). Russell (2002) contends that despite the significance of all three aspects – Technology People, and Process are essential in information security programmes, technical controls like firewalls and servers receive more attention, while processes and people are often overlooked. He notes that although these technical controls provide critical baseline defence, they can become ineffective if a user unintentionally or knowingly abuses their system access rights or fails to protect the information assets they control. As a result, special attention must be given to people, as they wield substantial influence over the failure or success of a cybersecurity programme.

2.3. DEVELOPMENT IN THE FINANCIAL SECTOR

Banking, as a concept, has existed for hundreds of years, continually evolving in response to societal needs. In the seventeenth century, banks began issuing banknotes, a practice that continues today (Davies, 2002). Goldsmiths in London stored gold in secure vaults for wealthy businesspeople for a fee. Based on the quantity and quality of the gold deposited, the businesspeople would receive a receipt. This receipt could then be used by depositors who

needed to spend the gold, allowing them to withdraw from the safe. Eventually, customers could use the receipt to make payments in shops. Paper receipts soon became viewed as equivalent to metal, marking the birth of paper money (Quinn & Roberds, 2009). Gradually, fiat currency replaced commodity-backed currency, with fiat currency no longer tied to gold (Rogoff, 2017). Automated Teller Machines (ATMs) appeared in the 1960s, with the first ATM emerging by the decade's end (Mayer, 2017). Banks heavily invested in computer-based technologies to automate much of the manual work, transitioning to automated systems (Gup, 2011). Payment systems developed in the 1970s, leading to electronic payment systems that support domestic and international payments (Carbo-Valverde & Rodriguez-Fernandez, 2003).

Governments worldwide collaborated with banks to foster the development of domestic payment systems. In the year 1973, the International Society for Worldwide Interbank Financial Telecommunications (SWIFT) payment network was founded (SWIFT, n.d.). The Royal Bank of Scotland introduced comprehensive internet banking services in 1997, allowing its customers to conduct various transactions through its website (Furst & Nolle, 2000). In 2007, The Royal Bank of Scotland became the first bank to introduce a fully functional smartphone banking app, enabling clients to perform fiscal transactions remotely using a mobile device (Ching & Ellis, 2004). In late 2008, Satoshi Nakamoto developed a secure, decentralized, peer-to-peer digital cash system called Bitcoin. This innovation laid the foundation for cryptocurrencies (Nakamoto, 2008). The system uses blockchain technology to issue currency, verify transactions, and process exchanges. As a decentralized currency, it is not controlled by a nation's central bank like regular fiat currency. The system is thus free from any manipulation or interference from governments (Narayanan & Goldfeder, 2016).

In the current computerised era, significant financial service transformations have occurred. The banking industry remained relatively unchanged for many decades, but the introduction of Fintech has prompted constant evolution, with many banks still struggling to keep up (Cytonn, 2019).

2.3.1. Evolution of Financial Technology (FinTech)

Financial technology is defined as the delivery of financial services enabled by technology. It represents the fusion of information technology and financial services. The interconnection between technology and finance has existed for a long time and is constantly evolving.

2.3.1.1. The History of FinTech

Technology plays a strategic role in enabling services in the financial sector. Arner et al. (2016) provide the following key periods in the timeline of fintech:

Table 2.1 Fintech Evaluation

	1866 – 1967 **FinTech 1.0**	1967 – 2008 **FinTech 2.0**	2008 – current **FinTech 3.0**	2008 – current **FinTech 3.5**
Geography	Global / Developed	Global / Developed	Developed	Emerging / Developing
Key Elements	Infrastructure / Computerisation Developed	Traditional / Internet	Mobile / Start-Ups / New Entrants	Mobile / Start-Ups / New Entrants
Shift Origin	Linkages	Digitalisation	2008 Financial Crisis / Smartphone	Last Mover Advantages

Source: Adapted from ZGIT (2022)

The significant events that took place in the periods outlined in Table 2.1, as described by Arner et al. (2015), are as follows:

i. Fintech 1.0 (1886–1967): From analogue to digital. This era is characterised by the global development of finance, with automation such as railroads, telegraphs, and steamships. These groundbreaking technologies marked the first instance of enabling swift cross-border transmission of financial information. This period saw the development of the first electronic fund transfer systems, i.e., the transatlantic cable in 1866 and the Fedwire, developed in the USA in 1918. This system relied on the Morse code and telegraph, which are now considered archaic technologies. In the 1950s, the advent of credit cards offered a convenient solution for alleviating the necessity of carrying cash. The inaugural credit cards, pioneered by Diner's Club in 1950 and subsequently by the American Express Company in 1958, brought about a transformative shift in the approach to financial transactions for individuals.

ii. Fintech 2.0 (1967–2008): The development of traditional digital financial services. This period is characterised by a change from analogue to digital. The first handheld calculator was launched during this time. In 1967, Barclay's Bank installed the first ATM, marking the dawn of modern FinTech. SWIFT was established in 1973, a

technology still in use today, facilitating payments across borders between financial institutions.

Online banking facilitated by bank mainframe computers was introduced in the 1980s. The penetration of e-commerce and the internet allowed online banking to prosper in the 1990s. Online banking revolutionised people's relationship with financial institutions and their perception of money. At the dawn of the twenty-first century, banks had been fully automated. This digitisation changed how banks interact with retail customers and outsiders, as well as their internal processes. This epoch concluded with the worldwide financial crisis in 2008.

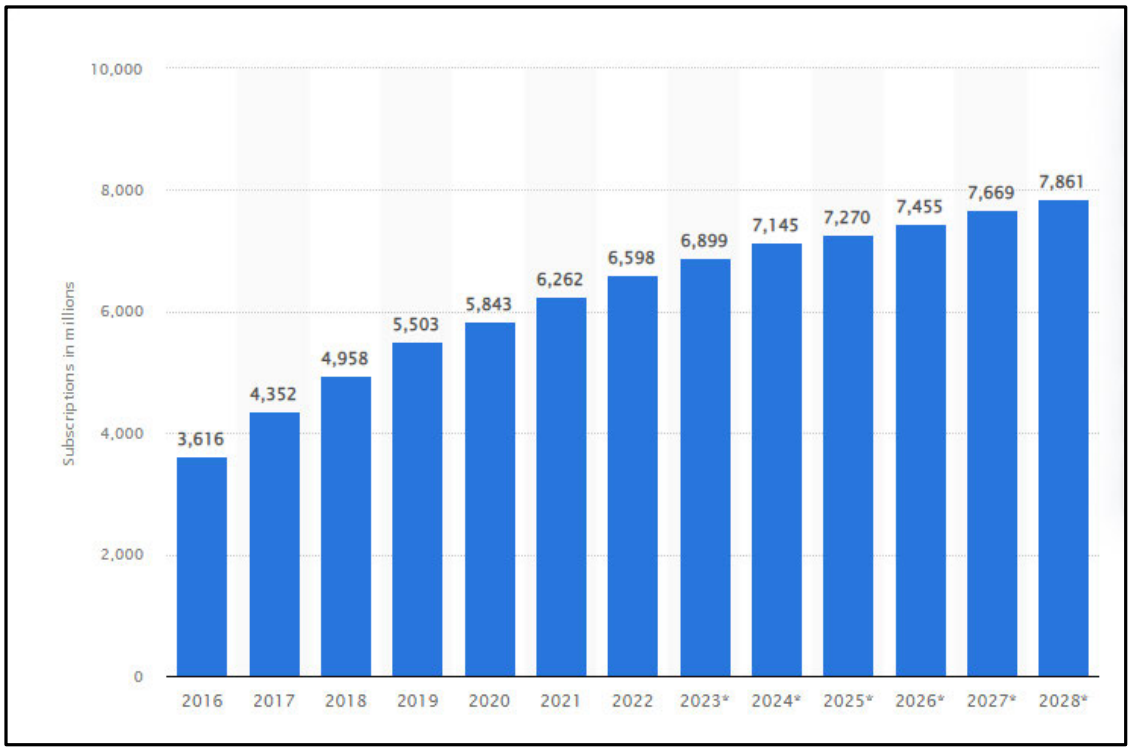
iii. Fintech 3.0 (2008–Current): Democratising digital financial services. The global financial crisis of 2008 triggered a far-reaching erosion of confidence in the conventional banking system. During the FinTech 3.0 era, novel players emerged, collaborating with existing stakeholders in the financial landscape. In 2009, the introduction of Bitcoin v0.1 had a profound impact on the financial world, triggering a subsequent surge in diverse cryptocurrencies.

The extensive proliferation of smartphones has exerted a substantial influence on the development of the FinTech industry, facilitating internet accessibility for millions of individuals across the globe. The growth and penetration of smartphones have made the smartphone the predominant channel through which people access financial

services and the internet. The growing global forecast in smartphone adoption is shown in Figure 2.2.

Figure 2.2 Global Smartphone Forecast for thePeriod 2016 - 2018

Source: Statistica (2023)



According to a report by GSMA (2021), the mobile services subscription rate in Sub-Saharan Africa reached 46% by the end of 2020, encompassing a significant number of 495 million individuals. This was an increase of 20 million people from 2019. As reported by the Pew Research Centre's 2019 Global Attitudes Survey, Kenya demonstrated a smartphone penetration rate of 30%. This positioned Kenya as the fifth-ranked country in terms of smartphone adoption, trailing behind South Africa with 51%, Ghana with 35%, Senegal with 34%, and Nigeria with 32%. In the first quarter of 2021–2022, a report by the Communication Authority of Kenya (CAK) (2021) indicated that the penetration of smartphones was 53.4%, while the penetration of feature phones was 67.9% in Kenya. This means that one in every two Kenyans owns a smartphone. According to the Q4 2020–2021 report by CAK, digital payments in Kenya increased by 21%, from Kshs 988 billion ($8.3 billion) to Kshs 1.2 trillion ($10.1 billion).

iv. Fintech 3.5 in Emerging Markets: The example of Africa and Asia. The emergence of mobile phones has significantly changed consumers' behaviour and their access to the internet. In Africa and Asia, Fintech 3.5 has been adopted primarily to pursue economic development, in contrast to Fintech 3.0 in the West, which was developed due to the financial crisis. According to the Global Fintech Adoption Index report by Ernest and Young (2019), India and China have the highest consumer Fintech adoption rate at 87%. The report suggests that India, China, and other growing markets did not have the time to develop the physical banking infrastructure seen in Western countries, which made them more open to new fintech solutions.

According to Arner et al. (2015), the emergence and development of Fintech 3.5 in emerging markets can be ascribed to various contributing factors, including the scarcity of physical banking infrastructure, the young population's digital savviness and ownership of mobile devices, inefficient capital and financial markets that create a market for informal alternatives, a fast-growing middle class, untapped market opportunities with over 1.2 billion people without bank accounts, a preference for convenience over trust, less stringent data protection and competition regulations, and a large number of graduates in technology and engineering in India and China.

Fintech 3.5 is the result of a combination of regulatory and entrepreneurial forces, with the public sector embracing market reforms to foster economic diversification and growth, and the private sector seeking to expand into financial services (Arner et al., 2015). In India, consumers have rapidly adopted Fintech due in part to the government's plan, announced in 2017, to reduce the use of paper currency (Ernest & Young, 2019).

2.3.1.2. Latest technologies adopted in the Kenyan financial services sector

The financial services sector in Kenya has experienced profound transformations, primarily fuelled by technological advancements. One outstanding exemplification of this transformation is the exponential growth of mobile money services.

2.3.1.3. Mobile Money

Mobile money refers to an electronic wallet service that facilitates users of mobile phones in storing, sending, and receiving money (Cytonn, 2019). In 2007, Vodafone and Safaricom, a local mobile network operator, jointly introduced the ground-breaking mobile money platform

called M-PESA in Kenya. M-PESA offers customers various monetary services, including deposits, loans, savings, and money transfers, and has gained countrywide adoption and acceptance. M-PESA is unique because it allows money to be transferred through Short Message Service (SMS), making it accessible to anyone with a phone, even those without smartphones.

Unlike developed nations, where online banking delivered through smartphones is more common, Vodafone and Safaricom recognized that most Kenyans, especially those in rural areas, did not have smartphones. In response, they invested in a service that was reliant on any phone. Within three years of its introduction, 70% of households in Kenya and 50% of the rural and remote population had adopted the M-PESA service (Zeisl, 2019).

Safaricom has since expanded its range of products by building on the success of M-PESA (Zeisl, 2019). In 2016, Safaricom unveiled the MySafaricom App, offering users seamless access to a wide range of Safaricom and M-PESA services in one convenient platform. Safaricom later added the Quick Response (QR) code scanning capability to facilitate payments. In 2017, Safaricom introduced the M-PESA app, empowering users to make swift and secure payments with a single tap through the utilisation of Near-Field Communication (NFC) technology. This innovative app supports various NFC-enabled devices such as NFC cards, Near Field Communication phone stickers, and Near Field Communication wristbands, providing users with convenient payment options. M-PESA has been highly accepted in Kenya and has since been embraced in Romania, Afghanistan, Tanzania, South Africa, and India.

The Communications Authority of Kenya's Q1 2021–2022 report (2021) shows that Kenya's mobile penetration stood at 59 million as of 30 September 2021. This figure indicates a remarkable penetration level of 133.3%, signifying that there are 34.6 million active mobile money subscribers, which accounts for an impressive 71% of the total population. During the quarter, 912 million Person to Person transactions valued at Kshs 1.081 trillion ($9.1 billion) were made, while customer-to-business transactions valued at Kshs 1.2 trillion ($10.1 billion) were transacted, representing a 7.1% and 21.1% increase, respectively. These statistics demonstrate an increasing trend in mobile money services, as shown in Table 2.2.

Table 2.2 Mobile Money Transfer Service for the Period July – September 2021

Service	No. of Agents	Total Active Subscriptions	Volume of P2P Transfers	Value of P2P Transfers	Value of C2B Transfers (Kshs.)	Value of C2G Transfers (Kshs.)	Total Value of Deposits (Kshs.)
Total	289,095	34,586,848	912,039,926	1,081,900,345,466	1,196,391,334,211	12,331,336,677	1,181,270,848,413
M-PESA	257,840	34,059,951	911,300,298	1,081,370,976,204	1,195,116,507,286	12,317,295,286	1,179,378,001,797
Airtel Money	22,197	277,143	302,581	402,575,469	1,227,534,204	13,998,806	1,852,959,029
T-Kash	9,058	249,754	437,047	126,793,793	47,292,721	42,585	39,887,587

Source: Adapted from CAK (2021)

Table 2.3 Growth in Mobile Payments

Year	No of Agents	Mobile Accounts (Millions)	No of Transactions (Millions)	Value (Kshs Billions)
2007	1,582	1.35	2.50	14.83
2008	6,104	5.08	62.74	166.57
2009	23,012	8.88	193.50	473.41
2010	39,449	16.45	311.05	732.22
2011	50,471	19.19	433.00	1,169.15
2012	76,912	21.06	577.37	1,544.81
2013	113,130	25.33	732.60	1,901.56
2014	123,703	25.25	911.34	2,371.79
2015	143,996	28.64	1,114.18	2,816.10
2016	165,908	34.96	1,331.01	3,355.11
2017	182,472	37.39	1,543.18	3,638.47
2018	205,475	47.69	1,739.57	3,984.37
2019	224,108	58.36	1,839.08	4,345.76
2020	282,929	66.01	1,863.30	5,213.54
2021	298,272	68.03	2,165.54	6,868.77

Source: Adapted from CAK (2021)

Table 2.3 presents a visual representation of the progressive development of mobile money services in Kenya, spanning from the initiation of M-PESA in 2007 to the year 2021. Table 2.3 encompasses crucial indicators such as mobile money subscriptions and agents' count, the cumulative total of mobile money subscriptions, the aggregate of mobile money transactions, and the corresponding transactional value across the specified years. The data displayed in the table unmistakably accentuates the swift and notable expansion of mobile money services within the Kenyan context.

Graphical representation of the data from Table 2.3 can provide a lucid and succinct portrayal of the growth of mobile money services in Kenya.

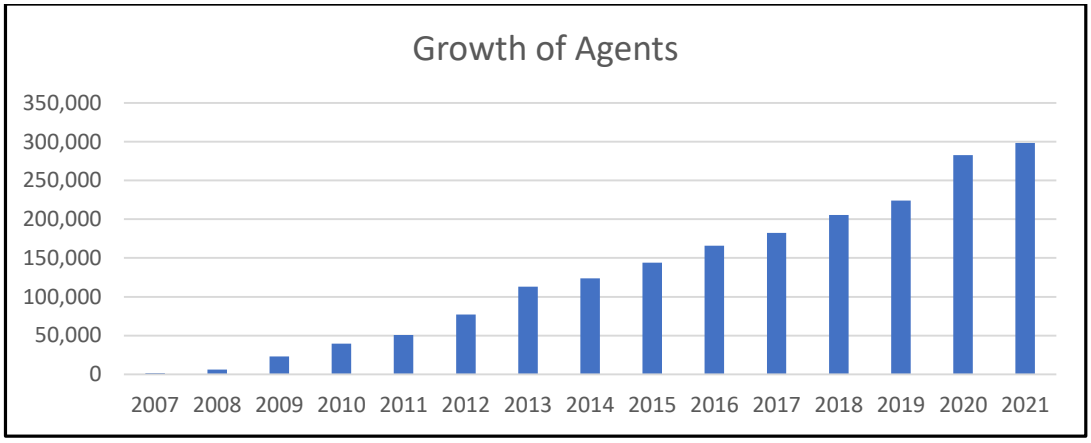


Figure 2.3 Growth of Agents

Source: Compiled by the Researcher

Figure 2.3 provides a visual representation of the progressive expansion of mobile money agents. These agents play a pivotal role in facilitating cash-in transactions for mobile money services, and their increasing numbers serve as a clear indicator of the widespread acceptance of mobile financial services across the country. By depicting the growth of mobile money agents over the years, Figure 2.3 effectively presents a concise and clear graphical representation of the growth of mobile financial services in Kenya.

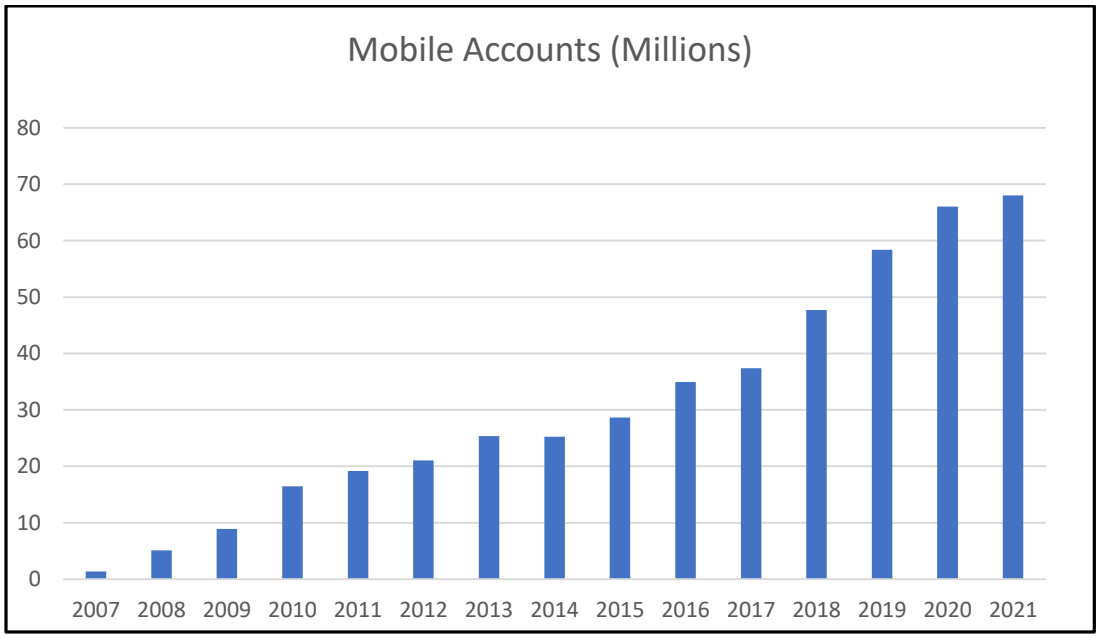


Figure 2.4 Growth of Mobile Accounts

Source: Compiled by the Researcher

Figure 2.4 displays a graphical representation of the rise in the number of users signing up for mobile financial services in Kenya. The graph provides a visual representation of the increase

in the utilisation of mobile financial services over time, confirming the growing acceptance of these services in the country.

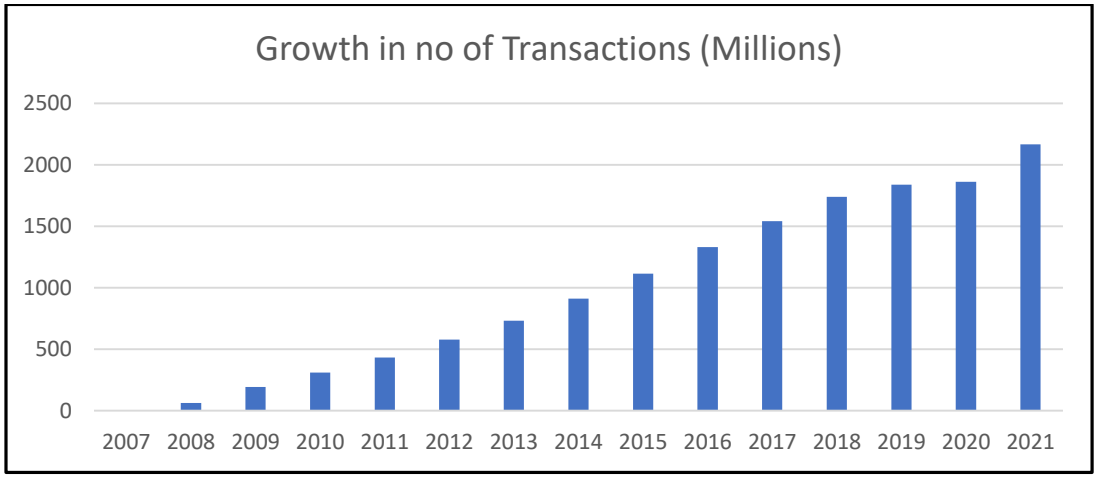


Figure 2.5 Growth of Mobile Transactions

Source: Compiled by the Researcher

Figure 2.5 presents a clear illustration of the escalating volume of mobile money transactions in Kenya from 2007 to 2021. The graph showcases a consistent and noteworthy growth trend, emphasising the ongoing and substantial rise in the adoption and utilisation of mobile financial services within the nation.

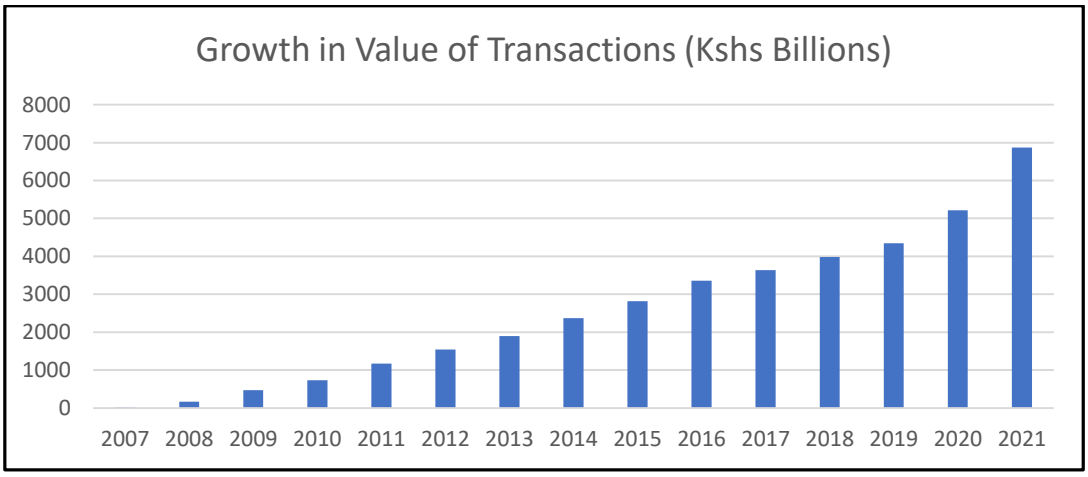


Figure 2.6 Growth in Values of Mobile Transactions

Source: Compiled by the Researcher

In Figure 2.6, a clear and continuous upward trajectory can be observed in Kenya's mobile money transaction values. The graph illustrates a gradual and consistent increase in transaction values over time, with a significant surge observed during the year 2021. This increase can be attributed to the government of Kenya's efforts to promote the adoption of digital payments and mobile money services.

2.3.1.4. Online / Internet Banking

Internet banking, also known as online banking, refers to an electronic payment system that empowers clients of financial institutions to conduct a wide range of financial transactions through either a dedicated smartphone application or the organisation's official website (Cytonn, 2019). The advent of online banking has brought about a reorganisation in the traditional banking system in Kenya, as illustrated in Table 2.4.

Table 2.4 Kenyan Banks' Transaction Volume by Channel

Name of Bank	Cooperative Bank	Equity Bank	KCB	Average	Combined
CBK Market Share Index*	9.9%	9.9%	14.1%		33.9%
Agency	32.2%	12.0%	20.0%	21.4%	
Mobile & Internet	28.1%	79.0%	55.0%	54.0%	
Branch	10.06	3.0%	12.0%	8.5%	
ATM	28.7%	4.0%	13.0%	15.2%	
Others	0.4%	2.0%		1.2%	

Source: CBK (2018)

According to Table 2.4, internet and mobile banking are the most active transaction channels, accounting for 54.0% of all banking transactions in Kenya. This has resulted in decreased activity in bank branches, which only account for 8.5% of all transactions. The utilisation of technology in financial services has led to improved efficiency and cost reduction for financial institutions. Nevertheless, the adoption of technology has resulted in a detrimental impact on employment, as it led to the closure of numerous bank branches and subsequently resulted in job losses. According to the Central Bank of Kenya's Supervision Report (2020), the efficiency score of the banking sector, calculated by the total number of deposit accounts per staff, has witnessed a remarkable improvement of 187.1% from 770 in 2014 to 2 211 in 2020. The growth in the banking sector can be attributed to the adoption of technology and a decrease in staff from 36 923 in 2014 to 31 605 in 2020, despite a 145.7% increase in the number of deposit account holders.

2.3.1.5. Digital Lending

Digital lending has experienced remarkable growth in Kenya in recent years (Cytonn, 2019). In 2012, the Commercial Bank of Africa (now NCBA bank after merging with NIC bank on 30 September 2019) partnered with Safaricom to introduce M-Shwari, a product that provides a savings account and access to digital credit. Since then, numerous players have entered the digital lending space, including the three largest banks in Kenya: Cooperative Bank of Kenya, Equity Bank, and KCB Bank, as well as FinTech and non-bank institutions.

The FSD Kenya Report (2021) reveals that Kenya has 49 digital credit providers, with M-Shwari and KCB-M-PESA accounting for 29% and 12% of the market share, respectively. Equity's Eazzy product represents 4% of the market share, while Tala and M-CooP Cash account for 1.8% and 1.3%, respectively. Digital credit services have substantially increased access to loans, allowing those without formal bank accounts or regular income to secure loans.

In January 2019, Safaricom, in partnership with the Commercial Bank of Africa and KCB Bank, launched Fuliza, a digital overdraft facility. Fuliza enables M-PESA users to carry out mobile payment transactions or transfer funds to other users, regardless of whether their M-PESA balance is sufficient. During the first week of its launch, the service saw an impressive uptake, with over one million M-PESA users signing up and collectively borrowing Kshs 1.0 billion ($8.4 million). A month later, 4.2 million customers had signed up, and a total of Kshs 6.2 billion ($52.1 million) had been borrowed.

The exponential growth in digital/mobile services offered indicates that these channels are gaining ground and providing efficient services, presenting a promising future for digital lending in Kenya.

2.4. GROWTH AND ADOPTION OF MOBILE FINANCIAL SERVICES (MFS)

Mobile Financial Services (MFS) pertain to the utilisation of mobile devices for performing financial transactions and accessing various financial services. These services assist many individuals with limited or no access to conventional banking services. The terms Mobile Financial Services and mobile money are often used interchangeably. Mobile money functions like a mobile wallet. A mobile wallet (mWallet) is akin to an electronic account on a mobile phone that functions similarly to a conventional wallet. It serves as a virtual storage space for money, enabling users to make purchases and conduct various financial transactions online (Mater, et al., 2021). Mobile wallets offer a versatile range of transaction channels,

encompassing consumer-to-business, consumer-to-online, consumer-to-consumer and consumer-to-machine interactions. These transaction channels enable users to engage in a variety of financial exchanges and activities using their mobile devices.

Mobile Financial Services represent a scalable and sustainable method for delivering affordable and convenient financial services to unbanked individuals (Ndung'u & Oguso, 2021). Mwangi and Kasamani (2017) contend that banking solutions and mobile phone-based money transfers offer an opportunity to bring financial services to people outside the traditional financial industry. They observe that this service has lowered the cost of accessing banking services for 2.3 billion people worldwide living on less than $2 per day, who cannot afford conventional financial services.

2.4.1. Classes of Mobile Financial Services

Mobile Financial Services can be broadly categorised into three main groups based on the services they offer.

i. M-Transfers: This category involves Peer-to-Peer (P2P) money transfers, where individuals can send and receive money to and from each other without the exchange of goods or services. These transfers can occur either within the same country (domestic P2P transfers) or across international borders (international P2P transfers).
ii. M-Payments: This type of service encompasses transfers between individuals, typically accompanied by the exchange of goods or services. M-Payments can be utilised for bill payments, Business-to-Business (B2B), Government-to-Business (G2B) or Government-to-Citizens (G2C) transactions.
iii. M-Banking: This service connects users to their bank accounts and offers various services typically accessed at a bank branch. M-Banking enables users to conduct various financial transactions, including transferring money between their bank accounts or to a mobile wallet. Users can make both domestic and international fund transfers. An example of this service is the partnership between M-PESA and Western Union in Kenya, which enables international transfers.

Table 2.5 Categories of Mobile Financial Services Available in East Africa

Category	Service	Platform Offering the Service
M-Transfer	Domestic money services	All mobile money platforms
	International money transfers from Western Union (currently, money flows one way to East African Community (EAC).	M-PESA Kenya
		MTN Mobile Money Uganda has a contract, but the service is not yet operational.
	Mobile Money users within EAC cannot send out international transfers).	M-PESA Kenya between Uganda and Kenya (informal)
	International transfers across EAC	
M-Payments	Buy airtime (on-network)	All mobile money platforms
	Pay post-paid phone bills	All mobile money platforms
	Businesses (customer to business, i.e., payments)	M-PESA Kenya (Nunua na M-PESA)
		MTN Mobile Money Uganda
		Airtel Money across EAC
	Bulk payments (business to customer, i.e., salaries)	M-PESA Kenya, M-PESA
		The United Republic of Tanzania
		MTN Mobile Money Uganda
		MTN Mobile Money Rwanda
	Utility providers (monthly bills for electricity, water, sewage, Pay TV)	All mobile money platforms
	Churches and NGOs (contributions)	M-PESA Kenya
		M-PESA The United Republic of Tanzania
		MTN Mobile Money Uganda
	Mobile ticketing (buy tickets for events, hotels, and airlines)	M-PESA Kenya
M-Banking	Mobile Money wallet linked to Bank Account	M-PESA Kenya (M-Kesho)
		Orange Money (Iko Pesa)
		YuCash Kenya
	ATM card Mobile Money withdrawals	M-PESA Kenya (Prepay VISA card)
		Orange Money (Debit card)
	Insurance (premiums)	M-PESA Kenya
	Microloans and repayments	MTN Mobile Money Uganda
		M-PESA Kenya

Source: Compiled by the Researcher[1]

[1] Adapted from operator websites.

2.4.2. Mobile Money Ecosystem

For a mobile financial service to function effectively, an ecosystem consisting of various interconnected players must exist. These players, who contribute to the successful operation of the service, are illustrated in Figure 2.7.

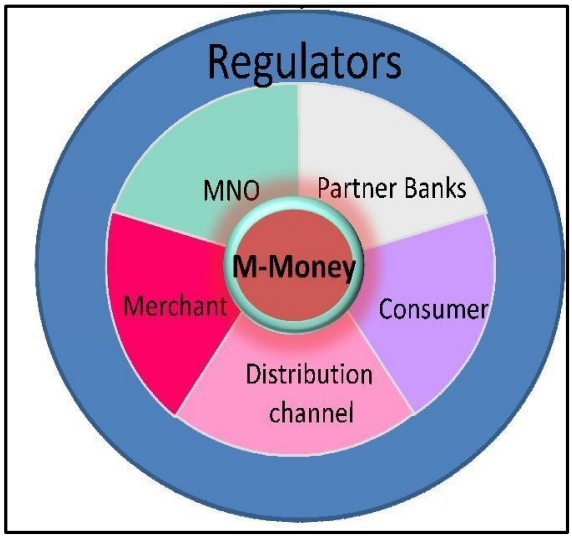


Figure 2.7 Mobile Money Ecosystem

Source: P. Tobin (2011)

2.4.2.1. Mobile Network Operator (MNO)

In the realm of wireless communications, a Mobile Network Operator (MNO) can be defined as a service provider that possesses or exercises control over all the fundamental components necessary for the seamless delivery of communication services to end-users. An MNO can be a cellular company, mobile network carrier, wireless carrier, or wireless service provider, offering telecommunications services to mobile telephony subscribers. In the ecosystem, the MNO supplies the assets and capabilities required for the infrastructure's functionality. This includes wireless communication, servers, and applications, as well as the distribution channel (agents).

2.4.2.2. Financial Institutions (Banks)

The function of financial organisations is to provide customer trust and expertise in financial matters. They contribute banking licenses and hold customers' money in trust accounts. As intermediaries between agents and banks in obtaining the e-value of money, they also offer advice on financial regulations to the mobile network operator. Tobin (2011) highlighted that mobile money enables banks to receive deposits more affordably than traditional methods. He

further contended that banks can generate additional revenue from deposits received through mobile money services.

2.4.2.3. Distribution Channels (Agents)

Agents play a pivotal role as the primary point of contact for customers. As non-bank entities, they perform customer registration and facilitate cash deposit and withdrawal services on behalf of the MNO. Essentially, they act as MNO branches. Agents are required to maintain sufficient liquidity to meet customer withdrawal requests and receive commissions for services provided on behalf of the MNO. Additionally, they provide informal training sessions to customers, educating them on how to utilise the services effectively.

2.4.2.4. Merchants and Utilities

These entities provide goods and services and accept payments from customers. As recipients of fund transfers, they could be utility providers of power or water, among others. They contribute to the adoption of MFS. Customers purchase value from agents and use MPESA (in Kenya) to send money to a merchant or utility provider's account. This service saves customers time by eliminating the need to wait in line at banks to pay bills.

2.4.2.5. Regulators

Regulators are responsible for balancing innovation, efficiency, financial inclusion, and value creation. They ensure compliance with regulations and mediate between competitors.

2.4.2.6. Customer

The customer brings their needs to the MFS ecosystem. The success or downfall of the ecosystem significantly hinges on customer satisfaction. Thus, it becomes paramount to diligently address and fulfil customers' needs, ensuring they have a positive and gratifying experience throughout their engagement with the services provided.

2.4.3. Typical Structure of Mobile Financial Service (MFS)

The range of services provided by MFS has continued to evolve. What started as a money transfer system has evolved to include M-Payments, M-Microfinance, M-Insurance, and M-Banking. It will, however, continue to evolve to include other services. A typical implementation involves the user, financial institution, MNO, and an agent. Ahirrao and Jethani (2014) provide the typical structure of MFS as presented in Figure 2.8.

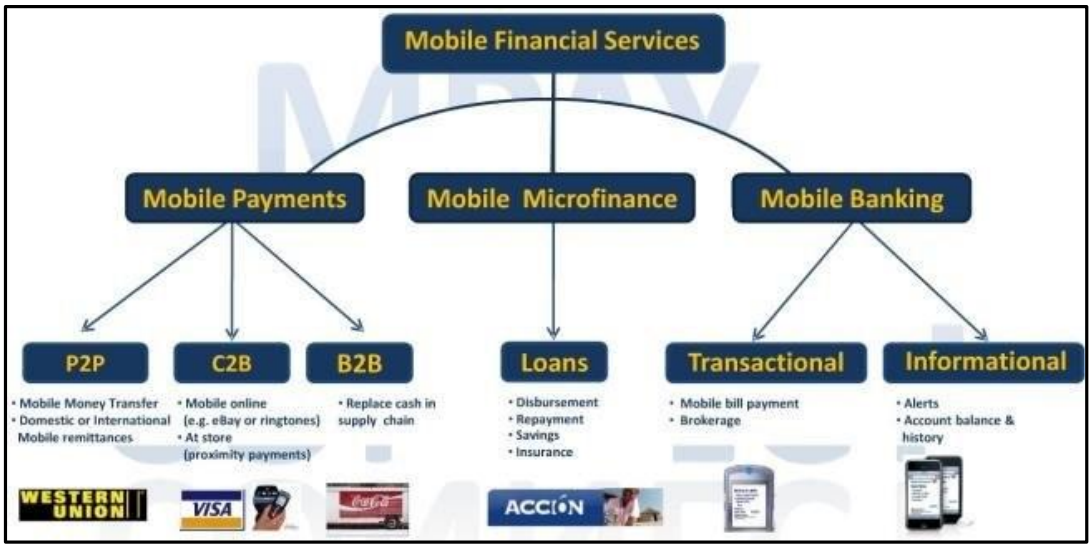


Figure 2.8 Mobile Financial Services Structure

Source: Ahirrao and Jethani (2014)

2.4.3.1. M-PESA System

M-PESA manages a system comprising low-value accounts maintained by the MNO. The system can be reached through the SIM card-based application on the user's mobile phone. Agents facilitate the conversion of cash and value within their shops. M-PESA system transactions are approved and documented instantaneously through a secure Short Messaging Service (SMS).

2.4.3.2. How the M-PESA System Works

To access the financial services offered by M-PESA, an individual must register at a distribution channel outlet and deposit cash. The customer must carry their identification documents, i.e., national identification card or passport. Agents use these documents to perform the Know Your Customer (KYC) on behalf of the MNO, a regulatory requirement. After registration, the customer hands over the cash to the agency staff, who deposits their money into a virtual account. The deposited amount is then displayed as e-money in a virtual account managed by Safaricom. Upon creating this account and establishing an e-money balance, a customer can use the M-PESA system to pay bills, transfer money to other M-PESA customers, transfer money to a bank account, or withdraw money from the bank to an M-PESA account. To obtain the e-money received via M-PESA, the customer must visit an agent outlet to withdraw the cash. The customer must produce an identification document at an agent outlet; the agent verifies the transaction reference and converts the e-money balance on their phone into cash.

2.4.3.3. Money Transfer Before the Advent of M-PESA in Kenya

Kenya is a developing economy, and most people with higher economic capacity are immigrants in urban areas. Often, they need to send money to the villages to support their relatives to pay medical bills, buy food, or send school fees for their siblings. If someone needed to remit money urgently back to their village, they would require finding a trusted individual who was traveling to their village at a suitable time (i.e., when there was a need to send the money). The person being sent must also be willing to pass by the sender's home to deliver the money or find a way of linking up with the family to deliver that money. Sometimes it would require the sender to call back home and inform them that he has sent someone with the money. Additionally, the one sent may take so long to deliver the money, and in some cases, they would use it or part of it. This process made money transfer tedious, insecure, painfully slow, and unreliable.

The same challenges were faced using other means of money transfer. Data from Financial Access Survey Report (2007) show that most people were using the hand delivery method to send money. A significant 58% of people sent money by hand, while only 3% sent it via someone else's account, who would then withdraw and pass it on to the recipient.

Table 2.6 Transfer Method

Method of Transfer	%
Hand	58
Bus	27
Post Office, Money order	24
Direct deposit	11
Money Transfer service	9
Cheque	4
Someone else's account	3

Source: Steadman Group (2007)

The success of mobile financial services has been linked partly to the limitations in dependability and scale of non-formal money transfer methods and the associated challenges. By the end of 2007, the same year Safaricom introduced M-PESA as a means of money transfer, the landscape changed as shown in Table 2.7.

Table 2.7 Method of Transfer

Method of Transfer	%
MPESA	47
Hand	32
Bus	9
Direct deposit	7
Other	5

Source: FSD Kenya (2007)

2.4.3.4. Hawala Money System

Hawala, meaning to transfer or trust, is a money transfer method without the physical movement of money. It can also be simply defined as "trust." Hawala is a channel that exists outside of conventional banking systems. This system has several names in different countries, for example, *havelah* in Persian and *xavala* in Somali. The transactions in hawala are based on trust and thus do not involve promissory notes.

2.4.3.5. Understanding Hawala

Hawala originated in South Asia in the eight-century CE to facilitate trade between Arabic and Muslim traders as an alternative means of transferring funds. The Hawala System is contrary to traditional funds transfer methods, such as bank wire transfers across borders. Hawaladars, or hawala dealers, facilitate money transfers in Hawala. Hawaladars maintain informal records of all debit and credit transactions on their accounts. Accounts between hawaladars can be settled through cash, services, or property. A hawaladar who does not keep their part of the deal in the hawala system will lose their honour and be excommunicated from the network.

The system aids the flow of funds between developing nations where conventional banking systems are difficult to access or too expensive. This system is convenient and fast, with a lower commission rate compared to those charged by banks. The system has proven advantageous for migrant workers who frequently send remittances to friends and family in their home countries. To encourage foreign exchanges through hawala, expatriates are sometimes exempt from paying fees by hawaladars. If one needs to transfer funds, they only need to find a trusted hawaladar to assist them, making the system easy to use.

2.4.3.6. How Hawala Works

Suppose customer A needs to remit $400 to B, who resides in a different city. The customer approaches hawaladar X and provides X with an amount of money B will collect, including the transaction specifics, B's name, passcode, and city. In the meantime, A sends a passcode to B and informs them about the money. X contacts hawaladar Y in the city where B resides and asks Y to give B $400, provided B correctly states the passcode. Y gives the money to B from their funds, minus commission, and X now owes Y $400. This transaction, initiated by A and finalised by B's receipt of the funds, may take just a few hours or, at worst, one to two days. Y is owed by X the money Y gave to B; Y must trust the promise by X to pay the debt later. There is no movement of money, and no promissory note is exchanged or signed by X and Y since hawala is supported only by trust, regional relationships, honour, or family connections.

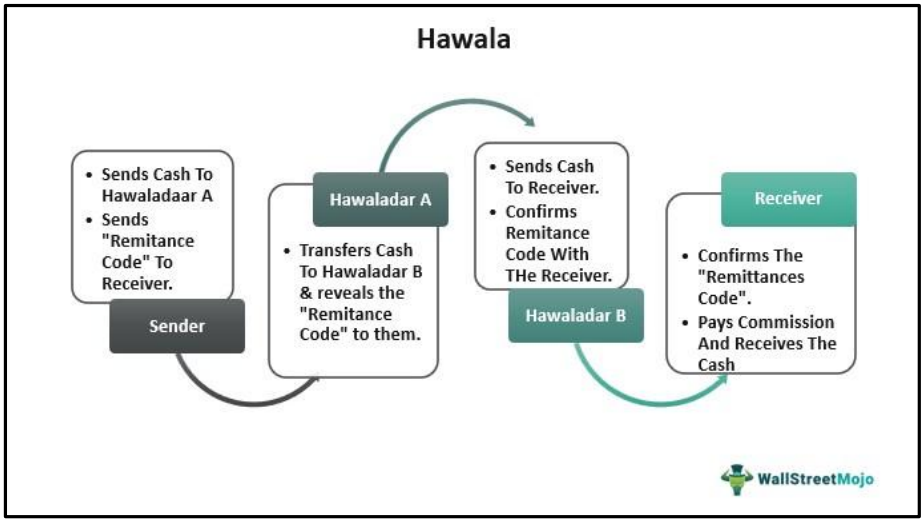


Figure 2.9 How Hawala Transactions Work

Source: Srivastav (2023)

Funds enter the hawala system in the sender's currency and exit in the recipient's currency. Since settlements can be made at non-official exchange rates, hawaladars can earn profits by bypassing official exchange rates in addition to the commission. What makes hawala an appealing path for lawful users also makes it attractive for illicit uses. This is because terrorists and money launderers use the hawala system to transfer money from one place to another. For this reason, hawala is commonly known as underground banking.

Hawala's lack of official records and the absence of regulation by governmental and financial institutions make it difficult to track the source of money in transactions. As a result, corrupt politicians and individuals who want to avoid taxes use hawala to conceal their activities and wealth. In response, many countries have re-examined their regulatory policies regarding

hawala. To combat the use of hawala, India has enacted the Prevention of Money Laundering Act (PMLA) and the Foreign Exchange Management Act (FEMA). These legislative measures serve as deterrents against illicit financial transactions and money laundering.

Despite these challenges, FinTech companies worldwide have either implemented or adapted the hawala system to offer financial services to the underbanked and unbanked populations. Mobile financial platforms, exemplified by Paga in Nigeria and M-PESA in Kenya, have brought about a revolutionary change in the financial system by promoting financial inclusion through their distinctive systems. Through harnessing the hawala concept and amalgamating it with contemporary technology, these platforms have facilitated seamless, rapid, and cost-effective money transfers and financial services for individuals who were previously constrained by limited or absent access to conventional banking systems. This innovative strategy has made substantial strides in promoting financial inclusion and driving overall economic growth within these regions.

2.5. INFORMATION SECURITY AND PRIVACY IN MOBILE FINANCIAL SERVICES

2.5.1. Information Security

Information Security refers to the implementation of systematic processes aimed at preventing unauthorised use, disclosure, access, disruption, inspection, recording, modification, or destruction of information (King, 2021). To ensure information security, organisations employ access control procedures through which authorised users can access a computer-based system while preventing unauthorised users from doing so.

Information security is a multifaceted procedure encompassing the regulation of information asset access to safeguard the principles of Confidentiality, Integrity, and Availability (CIA) of information to authorised users (Kim, 2022). The CIA-Triad serves as a foundational model guiding the formulation and development of information security policies within an organisation. The elements of the triad are the most critical in information security. The Security-CIA Triad is depicted in Figure 2.10.

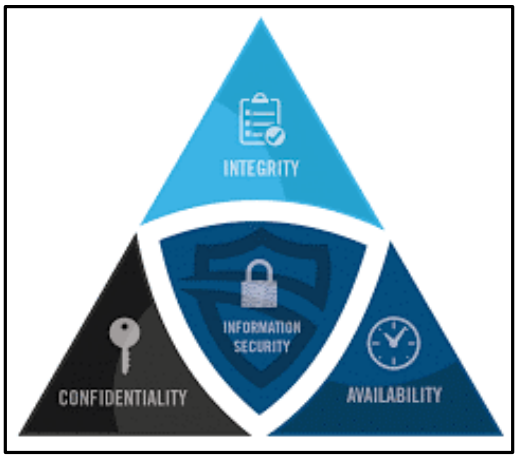


Figure 2.10 The Security-CIA Triad

Source: Preferred IT Group (2019)

Ham (2021) describes these three components as follows:

i. Confidentiality: These measures are specifically designed to prevent sensitive information from falling into the hands of unauthorised individuals while ensuring that the appropriate recipients have access to the relevant information.

ii. Integrity: This involves ensuring data consistency, accuracy, and trustworthiness during its life cycle. These measures aim to ensure that unauthorised people do not alter data.

iii. Availability: This means legitimate users can access the information when needed.

All attacks are crafted with the intention of compromising one or all these three fundamental information security principles (Russell, 2002). Whenever organisations evaluate new products or technologies, the CIA triad assists them in asking focused questions on how value will be provided in Confidentiality, Integrity, and Availability (Chai, 2021).

2.5.2. Information Security Issues in Mobile Financial Systems

The financial services industry is one of those at risk of cyber-attacks (Lagarde, 2018). Mobile devices have promoted customer mobility, heightening the risk of data breaches within Mobile Financial Services (MFS). The MFS industry must recognize the importance of the CIA triad to maintain growth and build customer trust and sustainability (Mazer, 2018). Bosamia and Patel (2019) identify several threats experienced by mobile financial services users, including:

i. Phishing attacks: Chanti and Chithralekha (2022) define these as fraudulent activities through which an attacker lures a user into stealing their credentials or personal information, using that information for financial gain.

ii. Social engineering: This concept refers to the act of deceiving and manipulating a user to illicitly obtain unauthorised access to information or a secure system (Steinmetz et al., 2022).
iii. Mobile operating system access permissions.
iv. Unintentional installation of rogue and malware applications.

Bosamia and Patel (2019) further identify the vulnerabilities of mobile financial services users, including:

i. Lack of user due care in authenticating content in messages and emails, and caution before downloading attachments or clicking links.
ii. Use of public Wi-Fi connections to perform mobile financial transactions.
iii. Use of fake websites.
iv. Use of non-genuine access points.
v. Downloading non-trusted files and installing non-trusted applications on mobile devices.
vi. Not adhering to minimum security hygiene rules.

Packer (2022) highlights some of the security concerns of consumers for not adopting mobile banking, as reported in a Consumers and Mobile Financial Services Federal Reserve report:

i. Data being intercepted.
ii. Device being hacked.
iii. Loss of a mobile device.
iv. Unauthorised device access.
v. Personal information used by organisations without authority.
vi. Malware installed on the mobile phone.

Financial institutions must consider several security factors, including mobile app assurance, mobile malware, Operating System (OS) and application trust management, access management, and customer identity and data protection. The successful implementation of these measures requires tactics such as mutual verification approaches incorporating multi-layered, multi-factor security procedures, for instance, two-factor authentication in a transaction that includes a one-time password or confirmations through SMS or call back.

There are three protection layers or levels where an attack on MFS can occur:

i. Device: Cyber attackers access the device through poorly coded mobile apps and steal sensitive data or personal information on the smartphone, which can be used for extortion.
ii. Transit: Intruders engage in the interception of sensitive information during data transfer. As the app continuously communicates with the bank server to update information, malicious actors can potentially obtain sensitive information during the transfer process if the protocol used for communication is not adequately protected.
iii. Server: Unauthorised users can gain access to the server through backend APIs if it has security vulnerabilities.

Attackers take advantage of mobile money applications in various ways (Surf, 2022), including:

i. Man-in-the-Middle (MiTM) Attacks: The intruder endeavours to intercept vital information during the transfer between the bank and the application, subsequently utilising the stolen data to compromise the user's account through hacking.
ii. Infrastructure Breaches: These attacks are directed towards servers with the primary goal of illicitly obtaining user credentials, such as passwords, usernames, and other personally identifiable information (PII).
iii. Pirate Apps: Intruders engage in reverse engineering of the mobile banking application, allowing them to create modified versions of the application. These altered versions are then distributed, and anyone who installs them becomes vulnerable to data compromise, as the intruders can use these modified applications to obtain sensitive user data.
iv. Mobile Malware: This term refers to malware specifically designed and targeted for smartphones.
v. Clickjacking: This technique involves enticing users to click on a button that triggers a malicious response, which may include downloading malware or collecting sensitive data without the user's knowledge or consent.

The Open Web Application Security Project (OWASP) mobile vulnerabilities report identified ten mobile security design flaws as highlighted by Surf (2022):

i. Improper Platform Usage: This issue arises due to the misapplication of operating system features or the failure to utilise the unique security features provided by Android

or iOS platforms. Failure to adhere to platform security requirements by the designer can lead to the exposure or corruption of app users' data.

ii. Insecure Data Storage: Internal data storage should be adequately protected to prevent access by malicious third-party applications.

iii. Insecure Communication: Mobile financial apps rely extensively on communication with external data sources, notably servers. However, in the absence of adequate security measures, this connection exposes the application to man-in-the-middle attacks or potential data leaks. To counter such risks, it is imperative to ensure encrypted communication using the Secure Socket Layer (SSL) protocol or other robust encryption algorithms.

iv. Insecure Authentication: This problem arises when a smartphone fails to accurately identify the user, thereby enabling an attacker to gain unauthorised access to the app through default credentials. To address this security vulnerability, developers must implement server-side authentication, refrain from allowing the app to store passwords on the device, and caution users about the potential risks associated with opting for the "remember me" feature. By adhering to these precautions, the app's security can be significantly enhanced, safeguarding sensitive user data from potential breaches.

v. Insufficient Encryption: Developers should give utmost priority to cryptography as a fundamental security technology, primarily due to its ability to render data unreadable, thereby providing a robust defence against unauthorised access. The implementation of strong encryption significantly increases the complexity of breaching data, requiring substantial amounts of time and processing power to attempt decryption.

vi. Insecure Authorisation: Authorisation determines which parts of the app a user can access based on their role. If the authorisation is well-designed, users will only have access to the data they have been granted. To circumvent insecure authorisation issues, it is essential not to solely depend on the permissions and roles impose by the mobile device. Instead, developers should implement a robust authorisation mechanism within the application itself.

vii. Poor Code Quality: Inconsistencies in the final code may occur when different developers within a team follow various development practices. This concern can result in heightened vulnerability for mobile app security, as it makes maintenance more intricate, potentially leading to security breaches and the presence of bugs. Standard practices for all members and proper documentation can help avoid this problem.

viii. Code Tampering: Attackers may change parts of the app's binary code, generate duplicates, and distribute these tampered fragments via third-party app stores. To thwart such malicious activities, developers must incorporate runtime detection mechanisms during the development process. This enables the app to identify any modifications or additions by comparing them to its known integrity at the time of compilation. Additionally, developers can implement an automatic erasure feature that wipes out the application's data and code as a response to any detected tampering.

ix. Reverse Engineering: Intruders may access the application code from the compiled file, allowing them to decipher the application's business reasoning. Developers have three options to avoid this:

    a. Use tools that attackers use for reverse engineering.
    b. Apply code obfuscation to make the source code more difficult to understand, reverse engineer, or analyse.
    c. Consider using languages like C and C++ that make the application resilient to tools used in reverse engineering.

x. Extraneous Functionality: Developers may retain code that does not have value for end-users but provides easy access to the backend server or creates logs for error analysis. These concealed functionalities have the potential to endanger sensitive end-user data. The approach is to test and remove unnecessary code from the final version.

The implementation of Mobile Secure Content and Threat Management (MSCTM) is imperative for establishing a safe mobile financial services experience for MFS users. The MSCTM strategy guarantees defence against hackers, spam, viruses, intrusions, spyware, and unauthorised disclosure or use of sensitive information (Weichbroth & Łysik, 2020; JT Force, 2020). Weichbroth and Łysik (2020) posit that vulnerability management and mobile security solutions help ensure the lockdown of devices, patching, and mobile device wiping. These solutions encompass aspects of mobile device security, including password policy management and compliance.

A secure mobile financial service experience necessitates a partnership between the provider and the user. While the service provider may implement multiple security layers, a weak PIN or conducting a mobile financial transaction over an unprotected Wi-Fi network can nullify the bank's efforts. The MFS provider must balance security with the critical need for a valuable and enjoyable customer experience. If it is too easy, it may be insecure, and if it is too hard,

customers will not use it. Employing a solution with multiple authentication factors has proven to be effective (Wang et al., 2023).

Global trends indicate that cybercriminals are becoming more sophisticated, and cyber breaches continually evolve, putting users at risk. Cyberattacks in the financial services sector initially targeted financial losses, but now the breaches are characterised by personal data loss (Shachmurove & McCulloch, 2021). The lost data can then be used to steal customer identities and commit fraud and other financial crimes. Cyber breaches may result in reputational damage, adversely affecting an organisation (Hasan et al., 2021). The repercussions of a data breach encompass the erosion of consumer confidence and trust, resulting in a decline in market share and potential scepticism towards new services and technologies that could have otherwise enhanced financial accessibility.

Mobile Financial Services have led to significant gains in financial inclusion. To protect and grow these gains, MFS providers must apply proper security controls to counter cyber-attacks. Mobile Financial Service users are primarily new to financial services and the technology that underpins the service. One of the most critical obstacles to theft through mobile devices is an alert and well-informed user (Jain et al., 2021; Hughes-Lartey et al., 2021). Therefore, awareness training campaigns must be developed for this group to ensure they can secure themselves and understand the associated risks with MFS.

Cybercriminals often target MFS users as the most vulnerable; thus, this human element becomes the weakest point of data security. Insider threats must also be considered since employees with access to systems can easily collaborate directly with cybercriminals. It is essential to build capacity and develop awareness initiatives among all those involved in delivering and using MFS to ensure the security of customer data.

Experiences such as falling victim to cybercrime hinder the development of Digital Financial Services (DFS) (Makin, 2018). This is especially true for low-income earners who cannot recover from such losses and those new to formal banking systems whose confidence in MFS is fragile. Makin (2008) notes that cybercrime has become a problem in developing countries, largely due to customers conducting financial transactions using unsafe mobile devices and communication lines not designed to secure financial transaction communications.

The key cyber threats in Africa encompass various types of fraud in cyberspace, including phishing, identity theft, and card-not-present frauds. The most common is phishing facilitated

by SMS, email, and phone calls (Interpol, 2021). Cybint (2020) adds that 95% of cybersecurity incidents are due to human error. Nduati (2018), in a survey commissioned by CGAP among 11 Digital Financial Service (DFS) providers in Africa, noted that all had been affected by cybersecurity incidents. From the survey, the four most common cyber threats in digital financial services were:

i. Internal fraud: Insider and third-party threats due to vulnerabilities in provider environments.
ii. Data breaches: Fraudsters using malware or social-engineering tricks to access sensitive customer information, like recent transactions and account types, enabling them to impersonate genuine customers and apply for credit in the victim's name.
iii. Identity theft. This arises when the Mobile Station International Subscriber Directory Number (MSISDN) of a subscriber is transferred without the explicit consent of the subscriber or knowledge from its current Subscriber Identification Module (SIM) card to another SIM card. Afterward, the fraudster takes control of the mobile number. The fraudster may obtain the customer's PIN by breaching the service provider's information system (through external or insider attacks) or via social engineering tricks.
iv. System downtime. This occurs during routine system patches or upgrades where service providers sometimes experience system outages. In 2017, during a system upgrade in Kenya, M-Shwari (a digital loan service by Safaricom, an MNO) customers could not access their loan products and savings for five days. Additionally, many customers had discrepancies in account balances after the disruption.

The Central Bank of Kenya (2019) developed a cybersecurity guideline for providers of payment services. The guideline requires organisations to formulate policies that specify suitable plans and mechanisms for incident response in the event of a breach and the appointment of a Chief Information Security Officer (CISO) to implement these controls and processes. The guideline emphasises the CISO's role in creating an organisational culture of shared cybersecurity ownership. These measures allow providers to meet their obligations on data protection, as prescribed by the data protection law.

Past and current efforts in cybersecurity awareness have failed to change user behaviour (Bada et al., 2019). Therefore, organisations must begin looking critically at challenges in improving the behaviours of employees and users. Changing behaviour might require not just information about risks and reactive behaviours but also understanding, motivation, and a willingness to

apply the advice (Bada et al., 2019; Zwilling, et al., 2022). Bada et al. (2019) suggest some critical factors that play a role in changing people's behaviour, including:

i. Personal Factors: This encompasses an individual's cybersecurity knowledge, skills, and comprehension, along with their experiences, attitudes, beliefs, and perceptions in the field.
ii. Cultural and Environmental Factors: These factors play a role in persuasion, as people prefer messages and advertisements that match their cultural themes.

Organisations should establish proper security procedures, both technical and organisational, that facilitate adaptability and help ensure the business maintains enterprise-wide compliance, keeping pace with changes in regulations (Gebel, 2019). To achieve this, MFS should not just focus on introducing appropriate technical systems but must adopt a comprehensive strategy that encompasses technology, processes, and people.

2.5.3. User Responsibilities in Information Security

Managing user behaviour is an ongoing process for management in numerous organisations. This is particularly critical in the information security domain, where unintentional actions by a user can seriously affect an organisation's information security posture (Ogbanufe, 2021). Users with legitimate access to organisational information resources for their daily tasks can inadvertently or deliberately compromise the information security endeavours of their organisations. Such actions can lead to substantial financial or legal losses if they fail to comprehend their roles in safeguarding those information assets (Altamimi, 2022). To avert such undesirable incidents, users should be knowledgeable about the potential harm and the safeguards they need to implement to mitigate them (Koyuncu & Pusatli, 2019).

IBM (2023) identifies the following responsibilities which every user must be aware of, understand and follow:

i. Set passwords and keep their passwords private (confidentiality).
ii. Do not store passwords and usernames on mobile phones.
iii. Report information security violations.
iv. Report changes in their status.
v. Restrict use to authorised purposes.
vi. Comply with organisation policies.
vii. Comply with federal and state law.

viii. Accept accountability for their user accounts.
ix. Log off or lock workstations / mobile devices when not in use or unattended.
x. Ensure that visitors and vendors are escorted whenever they come to one's department.
xi. Do not install unknown software.
xii. Avoid unauthorised disclosure of data on computing devices.
xiii. Protect confidential or restricted information.
xiv. Dispose of confidential or restricted information securely.
xv. Users should ensure they maintain an up-to-date antivirus software.
xvi. Users must not open email attachments from unknown sources.
xvii. Users should verify attachments from known sources and scan with an antivirus before opening.
xviii. Users should not open unknown/suspicious links or websites.
xix. Ensure the system is up-to-date and get updates from vendor-provided sites.

In the first-quarter report by the Communications Authority of Kenya (2021) for the period July-September 2021, the national point of contact entrusted with cyber security issues in Kenya, the National KE-CIRT/CC, detected the cyber threats incidences as depicted in Table 2.8.

Table 2.8 Cyber Threat Incidences

Cyber Threat	Jul-Sep 2021	April-June 2021	Quarterly Variation (%)
TOTAL	143,040,599	38,776,699	268.9
Malware	70,501,144	23,053,190	205.8
DDOS/Botnet	49,816,062	11,272,402	341.9
Web Application Attacks	478,123	2,564,173	-81.4
System vulnerabilities	22,245,270	1,886,934	1,078.9

Source: CAK (2021)

The significant increase in cyber threat attacks, as shown in the report in Table 2.8, highlights the growing challenges faced by users and organisations in ensuring the security of their financial transactions and data. In developed countries, financial providers are often responsible for covering the costs of fraud. However, in developing countries, the clients themselves bear the brunt of these costs (Baur-Yazbeck et al., 2019).

The discrepancy can potentially result in diminished confidence in digital financial services, particularly among low-income users who are already more susceptible to fraudulent activities (Aziz & Naima, 2021). The experience of fraud, or even hearing rumours of such incidents, can create a sense of insecurity and discourage people from adopting and using digital financial services. This lack of trust can impede efforts to foster financial integration and improve access to banking services in developing countries.

To address these challenges and build trust among users, it is crucial for organisations, governments, and regulators in developing countries to establish robust cybersecurity frameworks and invest in awareness campaigns that educate users about safe mobile money practices. Additionally, there is a need to develop policies and regulations that hold financial providers accountable and ensure that they implement adequate security measures to protect their clients' data and assets. By taking a proactive approach to cybersecurity and creating an environment of shared responsibility, it is possible to foster trust in digital financial services and promote their adoption among low-income users.

Therefore, the increase in cyber criminality means the users need to know the risks associated with MFS and adopt good security practices. Ali et al. (2020) suggest some good behaviours that are an essential step toward the safety of mobile money, including:

i. Lock for the mobile device: This could be a PIN/Password or an app that provides a lock or unlock feature. This app can also help lock the phone when it is lost or stolen.
ii. Need to ensure the mobile apps are safe and legitimate: The golden rule is downloading apps from trusted sites. Additionally, it is vital to check the app ratings and reviews from other users and read the permission requests before downloading.
iii. Users need to use mobile payment applications that issue immediate receipts. This helps one to follow up on transactions in your mobile or bank account.
iv. Users need to turn off Bluetooth or Wi-Fi when not in use.
v. Always keep the Operating System (OS) of the phone up-to-date and not unlock the phone's operating system to allow installation of unapproved apps or replacing the phone's firmware. If the phone's OS is unlocked, it becomes vulnerable to exploitation by malware and hackers who can then steal one's financial data or intercept messages.

It is everyone's responsibility to ensure that information systems are secure. Therefore, every user interacting with organisational systems using digital devices should remain vigilant and take security precautions to protect information assets.

2.5.4. Security Theatre in Cybersecurity

Organisations that have appreciated cyber-attacks and data breach risks have invested colossal sums of money in software and technologies to protect their networks and systems (Schlackl et al., 2022; Armenia et al., 2021). Security theatre thereby proves that it is increasingly vital for organisations to differentiate between policies and measures just for display and those that genuinely aid in detecting, preventing, and containing data breaches and cyber-attacks.

Porup (2020) highlights a few examples of theatrical security measures that do not make systems safer, including:

i. Splash screens: Examples can be seen when doing online transactions, and after login, the page shows "setting up a secure connection" or "securely getting your connection." Unfortunately, these messages are displayed in a flash, and if the flash blocker turns them off, one will realise it was pointless to have them in the first place.
ii. Antivirus and Antimalware Software: Having antivirus software is baseline protection for digital devices. However, it is not the end since installing malware can still lead to performance degradation. Some malware today is built with antivirus payloads that bypass protection as if it did not exist.
iii. Perimeter security: Firewalls and perimeter walls are theatrical practices that do not make enterprises secure anymore. Many gates have been stormed, and the firewalls cannot promise to keep the attackers out anymore. Since many enterprises are in constant breach, there is a need to have new strategies and technologies. An example could be to invest more in Disaster Recovery Plans (DRP) so that in the event of a breach, the organisation can detect, minimise impact, and recover quickly by setting up shorter backup periods.
iv. Alert fatigue: Installing security products that send many alarms, but nothing is done about it is a security theatre. Studies show that IT teams only investigate 5% of incidences that trigger the alarms (Sobers, 2022). Some threat protection products send out alarms which turn out to be false positives.
v. Ignoring what your gear tells you: Many organisations have bought and implemented security equipment like Intrusion Prevention Systems (IPS) and firewalls but rarely look at the data these devices are capturing.
vi. Complex Password Requirements: This is the most visible security theatre. One is required to enter a password, but once one gains entry, there is no additional protection.

Secondly, this is a weak link since most users prefer to use passwords that are easy to remember than one that is hard to decipher. Additionally, the requirement to change passwords after a period is another theatre since some opt to change the last digit.

vii. Security training: Sending out simulated phishing attacks every so often with no prior interactive, engaging user training that explains the risks leaves users hassling and does not decrease phishing attacks. Additionally, security awareness and training should not be tedious and burdensome. Trainers must rethink how information and content in these training sessions are presented. They must endeavour to engage and interact with users by showing them how everyone benefits from security and their role in improving organisational security.

viii. Tough talk: Installing a device sold by a company describing the encryption it gives as "military-grade encryption" does not necessarily result in secure systems.

ix. Stonewalling: When the IT team rejects a request to access a resource from a user by simply saying it comprises security without figuring out how to grant such access securely is theatrical.

x. Information sharing: Sharing data about data breaches experienced may amount to performance as well. While sharing data about breaches might help the organisation patch the systems, it does not do anything about exposing hidden attackers that might make organisations feel secure while they are not.

A feeling of security occasioned by security theatre and being secure because of effective security are two different scenarios whose difference is shown in cybersecurity.

Security theatre loves the stage and primarily comprises procedures, tools and technologies that only show an organisation's superficial security (Jelen, 2019). The author posits that security theatre focuses on the expression of security but fails to equate the actions with the risk sources. This leaves the organisation with a hole in the budget and organisation systems vulnerable to hacking. Therefore, organisations must continually review the effectiveness and reliability of their cybersecurity approaches; otherwise, they will remain exposed to data breaches and malware (Jelen, 2019).

Successful cybersecurity measures utilise a risk-based perspective to cybersecurity practises. It involves the identification of all-important organisations' digital assets, identifying weak points and finally, building the organisation's defences appropriately (Kaminski et al., 2017;

NIST, 2021b). Achieving this requires the cybersecurity staff to remain appraised about the latest cybersecurity situation and defences in the organisation.

Some measures to guarantee effective cybersecurity involve monitoring privileged accounts and third-party access, raising user awareness, and enforcing proper email security (Ekran, 2022). These practices and procedures do not look flashy but go a long way to decrease the organisation's chances of becoming another statistic in data breaches.

The process of analysing to determine the risks, providing mitigation to those threats, and building defence strategies are among the approaches to exchange "feeling secure" for actually "being secure" (Jelen, 2019).

2.5.5. Impact of Security Theatre in Creating Effective Security

Schneier (2003) defines security theatre as the practice of organisations investing in countermeasures aimed at creating a sense of improved security, yet these measures often make little to no tangible progress towards achieving the actual desired level of security. Schneier, a cybersecurity expert, initially coined the term "security theatre" to describe airport practices such as removing shoes, limiting fluid volumes, and other measures intended to project an image of a secure environment without improving overall security. These countermeasures and actions create a sense of security for individuals without truly enhancing it (Schneier, 2003).

The term now applies directly to numerous technical security measures that many organisations have implemented but do not guarantee their information security. Today's organisations enforce numerous security protocols and insufficient measures to prevent future cyberattacks. Consequently, organisations will continue to be at risk of data breaches and malware if they do not constantly review the effectiveness and reliability of their cybersecurity approaches (Nobles, 2022; Jelen, 2019).

Globally, the occurrence of cyber threats has witnessed a rise in both quantity and intricacy. Almost daily, headlines feature new data breaches, emphasising the urgent need for cybersecurity awareness training. Jennings (2022) highlights the Top-10 most significant data breaches and cyberattacks. The list includes large organisations such as Microsoft, News Corp, Red Cross, Uber, and Pressreader. Successful attacks on these organisations systems demonstrate that malicious actors are always ready to exploit weak security practices and vulnerable data (Jennings, 2022).

A study conducted by Michel Cukier at the University of Maryland's Clark School revealed that cyberattacks occur every 39 seconds (Cukier, 2007). According to a report from Netscouts, Internet of Things (IoT) devices experience attacks within a remarkably short timeframe of just five minutes after being connected to the internet (NetScout, 2019). Another report by Kaspersky (2022) reveals that small businesses in Kenya continue to be at risk of cyberattacks, experiencing a 47% increase in internet attacks, with 88 455 attacks recorded from January to April 2021 and 130 111 infections occurring within the first four months of 2022. As per the IBM Security Cost of Data Breach Report (IBM, 2022a), data breaches now incur an average cost of $4.24 million, which represents a 10% increase compared to the figures reported in 2019 ($3.86 million). These statistics are prompting organisations to prioritise cybersecurity and allocate more of their IT budgets to technologies that ensure adequate protection of their information assets.

The pressing question is whether these efforts are yielding results. Are antivirus software and firewalls effectively safeguarding from cyber threats, or are they simply unnecessary budget expenses? In other words, do the invested measures provide only a superficial sense of security rather than genuine cyber risk mitigation (Jelen, 2019)? While security theatre relies on the psychological feeling of security, the actual security process depends on the likelihood of diverse risks and counter-measures' efficiency. Since security theatre is based solely on emotional reactions, individuals may feel safe, when, in fact, they are not secure.

It is worth noting that security theatre measures may have positive effects as well. For example, security theatre measures can help alleviate cybersecurity stress on an average user's mind, enabling them to assess threats more rationally. However, people may become complacent and feel too comfortable when given a false sense of security. Some real-life examples of security theatre include:

i. Security guards at airports confiscating liquids, while terrorists could potentially cause damage using solids.
ii. Prohibiting bottled water on flights because it exceeds a specific volume yet allowing flammable aftershave.
iii. Body scanners that appear high-tech but do not perform better than traditional ones.
iv. Urging people to report any suspicious activity, which serves only to make them suspect one another and further increases their sense of helplessness and fear.
v. Requiring facility access with ID badges that can be easily duplicated by criminals.

vi. Displaying stickers in cars and homes, announcing they are protected by security camera monitoring or a sophisticated theft deterrent system.

Certain measures have the potential to enhance security, such as the use of warning stickers on homes, which may act as a deterrent to potential thieves. However, it is worth noting that these measures can be susceptible to circumvention.

Security theatre typically alters or restricts people's environments or behaviours in conspicuous and distinctive ways (Mann, 2011). The author notes that security theatre may sometimes have no tangible monetary costs but offers no security benefits, or the gains are so minimal that the expense is not justified.

The immediate cost of security theatre may not be significant. However, the danger lies in potentially diverting portions of the budget that could have been used for effective security measures without providing a measurable and reasonable improvement in information asset security (von Skarczinski et al., 2022; Herath et al., 2022).

2.5.6. Privacy

Privacy is a component of information security that encompasses proper data handling, including consent, necessary notices for managing client data, and regulatory obligations (Buckbee, 2023). Data privacy concerns itself with aspects such as:

i. The way data is distributed to third parties, if at all.
ii. The lawful collection and storage of data.
iii. Regulatory provisions like the Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), Gramm-Leach Bliley Act (GLBA), and the General Data Protection Regulation (GDPR).

It is crucial to note that ensuring sensitive information is secure from intruders does not automatically guarantee compliance with data privacy regulations (Buckbee, 2023). For instance, an organisation might have secured Personally Identifiable Information (PII) effectively through encryption, limited access, and multiple overlapping monitoring systems. However, if the data owners' consent was not obtained before collecting this PII, the organisation is likely violating a data privacy regulation, even though the data is secured.

This implies that an organisation cannot have data privacy without data protection, although data protection can exist without data privacy.

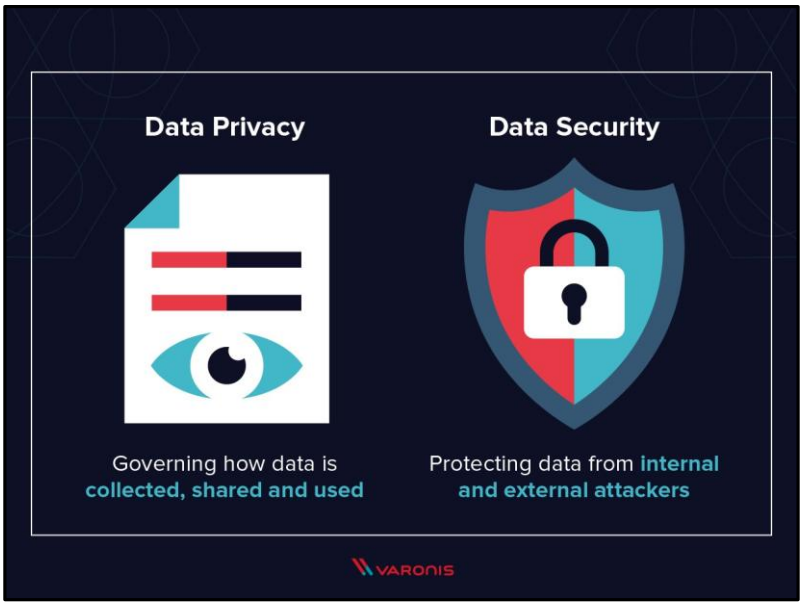


Figure 2.11 Privacy: Data Privacy vs. Data Security

Source: Buckbee (2023)

Data is vital to many organisations, necessitating transparency in obtaining user consent, adhering to privacy policies, and managing collected data. This transparency is essential for enhancing accountability and trust with partners and customers who expect privacy (Buckbee, 2023).

Ensuring data privacy means that organisations refrain from indiscriminately collecting personal data about customers, whether through surreptitious location tracking, apps that covertly access customers' address books, or websites that record every keypress by customers.

Information privacy comprises the regulations organisations must follow to ensure data protection (Buckbee, 2023). The author emphasises that data protection regulations and global privacy requirements are evolving and expanding worldwide. Amid these changes, adequate data protection remains a constant, helping organisations comply with legislation while ensuring information privacy (Buckbee, 2023). Continuous training in data protection is imperative to gain a comprehensive understanding of the processes and procedures involved in the appropriate collection, sharing, and utilisation of sensitive data.

Privacy concerns are particularly critical for organisations in the healthcare and financial sectors (Swinnen, 2020). This is primarily because banks and other financial institutions handle vast amounts of sensitive client information, and breaches of such data can have far-reaching consequences (Swinnen, 2020). Tobin (2021) asserts that data privacy concerns have

increased as organisations conduct financial transactions online and store information in the cloud.

Several laws, including GDPR, CCPA, and HIPAA, have defined data privacy in different ways. However, these regulations underscore the rights of businesses and consumers and recommend best practices for ensuring data privacy.

2.5.6.1. Data Privacy Laws and Acts

Figure 2.12 Data Privacy Law and Acts Timeline

Source: Buckbee (2023)

The Kenya Data Protection Act and GDPR are examined in the following sections.

The General Data Protection Regulation (GDPR)

The GDPR (Burgess, 2020) was implemented on 25 May 2018, replacing the Data Protection Directive of 1995. Its primary objective is to safeguard the personal data of European Union (EU) citizens. The regulation requires companies to undertake several tasks to comply with the GDPR. Some of these tasks include:

i. Obtaining authorisation from users
ii. Allowing users, the right to request data from organisations.
iii. Providing the right for users to have their data deleted.

The major provisions of the GDPR include the following:

i. Extra-Territorial Nature: It applies to any organisation that processes personal data, even if the server processing the data is not in the EU. Furthermore, the GDPR extends its applicability to businesses located outside the European Union (EU) that handle the personal data of EU citizens.
ii. Appointment of Data Protection Officer (DPO): The DPO's role is to offer counsel to organisations on their obligations under GDPR and monitor compliance. Under the regulation, organisations must decide whether to appoint a DPO. However, a DPO must be appointed by the following:
    a. Public organisations.
    b. Organisations dealing with extensive processing of specific classes of personal data (e.g., PII revealing ethnic or racial origin, political opinions, genetic information, health information, and religious beliefs) or related to criminal offenses.
    c. Organisations dealing in extensive systematic and regular monitoring of individuals.
iii. Consent: Organisations must demonstrate they have received valid consent from individuals whose data is to be processed to lawfully process such personal data. This permission must be granted willingly, informed, unambiguous, specific, and in plain language. Moreover, individuals should retain the right to withdraw their consent at any time, and this process of withdrawal should be as straightforward as providing consent initially.
iv. Enhanced Rights of Individuals: The regulation grants individual's various rights regarding their personal data, which include the right to access, rectify inaccuracies,

request erasure under specific circumstances, restrict processing, exercise data portability, object to data processing, and avoid automated processing, including profiling.

v. Reduced Period to Address Individuals' Rights: Organisations must provide appropriate information without delay and within one month should an individual make a request. This period was reduced from 40 days to one month and can be extended if the requests are numerous or complex.

vi. Clarity on Personal Data Use: Organisations are strongly encouraged to adopt a transparent approach regarding the utilisation of personal data. This entails presenting such information in a concise, intelligible, and transparent manner that is easily accessible to individuals. The communication should utilise clear and straightforward language. In cases where the data processing concerns a child, the information should be conveyed in a language that can be easily understood by a child.

vii. Data Protection Impact Assessment (DPIA): Organisations should evaluate the impact of the assessment on personal data, particularly if the processing poses a high risk to an individual's rights.

viii. Data Breach Notifications: In case of a personal data breach, the regulation mandates that the Data Protection Authority (DPA) must be notified within 72 hours of becoming aware of the breach, unless it is determined that the breach does not pose any risks to the rights of individuals. If the breach will result in risks to individuals' rights, the regulation provides for their immediate notification in clear and plain language.

ix. Data Protection by Design and Default: The regulation demands that organisations take proactive steps to implement measures that uphold data protection principles and integrate appropriate safeguards into their data processing practices. These measures should be designed to ensure compliance with GDPR requirements and uphold the rights of individuals, safeguarding their personal data.

x. Right to Individual's Compensation: Any person who has suffered harm due to a GDPR infringement must be compensated by the organisation for the harm suffered, unless the business can prove it was not responsible for the event that caused the damage.

xi. New Obligations for Processors: The regulation establishes a new equilibrium between data processors and data controllers, making them severally and jointly liable based on

their corresponding responsibility for the damage resulting from a breach of data protection law.

xii. Increased Penalties: The regulation has increased the fines for non-compliance with GDPR provisions.

xiii. Ability to appoint a Lead Supervisory Authority (LSA): The DPA is responsible for enforcing GDPR. However, organisations operating in multiple EU countries should nominate the LSA, whose responsibility is to deal primarily with complaints and queries concerning cross-border processing. The Lead Supervisory Authority should be a DPA in the European Union country in which the business has its headquarters.

The regulation imposes security obligations on organisations responsible for holding consumer data, while concurrently empowering consumers with rights over their own data. This includes the right to make data subject access requests, which organisations must respond to promptly. Nevertheless, the task of quickly locating, providing, or deleting an individual's personal data upon request can be challenging for many businesses. To address this, numerous Data Protection Officers (DPOs) and Chief Information Officers (CIOs) rely on GDPR-compliant software that facilitates automatic discovery and classification of personal data. Such software aids in safeguarding personal data and expediting responses to access requests from data subjects.

Kenya Data Protection Act (2019)

The Kenyan government enacted the Data Protection Law, 08 November 2019, which became effective 25 November 2019 (Government of Kenya, 2019). This Act governs the collection and processing of data in Kenya and delineates the responsibilities of individuals who gather and process data, as well as the penalties for noncompliance. It has been considered a significant milestone in data protection.

The legislation creates the Data Protection Commission, led by a Data Commissioner appointed by the president with the concurrence of the National Assembly. The responsibilities of the Data Commissioner include operationalising the Act, maintaining records of data processors and controllers, overseeing data processing operations, and handling complaints related to rights infringement as outlined in the Act.

The Act is applicable to both data controllers and processors, irrespective of their geographical location, provided they engage in processing personal data within Kenya or manage personal

data pertaining to individuals located in Kenya. The Data Commissioner is vested with the authority to conduct periodic inspections of the systems and processes employed by data processors and controllers to ensure strict adherence to the provisions outlined in the Act.

The Act delineates data protection principles based on the GDPR principles. It outlines the rights of individuals providing their personal data, which include:

i. Being apprised of the intended purpose for their personal data.
ii. Having access to their personal data granted by the data processor or controller.
iii. Having false or misleading data about them corrected or deleted.

The Act stipulates those certain conditions, as defined in the Act, must be met before personal data is processed. These conditions include obtaining the permission of the individual whose data is being processed. Moreover, the Act prohibits processing sensitive personal data except for authorised reasons, as specified. Additionally, only a healthcare provider can process an individual's health-related personal data under the authority of the healthcare institution or by an individual bound by professional confidentiality under any law.

The Act mandates that one's personal data should not be used for commercial purposes unless approval has been obtained from them. It is essential to recognize that privacy concerns among Kenyans before enacting this law included unsolicited marketing messages from organisations, uninformed misuse of personal data, and the requirement for individuals to identify themselves and record their identification documents at building entrances.

The impact of this Act is that organisations collecting, controlling, managing, and storing data must assess the provisions in their terms and conditions and activities to mitigate the risks arising from noncompliance with the law.

In conclusion, both the Kenya Data Protection Act and GDPR share the common objective of regulating the processing of personal data and protecting individuals' privacy rights. While there may be variations in specific provisions and requirements, organisations operating in these jurisdictions must ensure compliance with the respective data protection laws to avoid penalties and maintain trust with their customers and partners.

Legislators have acknowledged the importance of having regulations on data privacy and the critical need to hold organisations accountable for customer data. Organisations must, therefore, identify which privacy laws affect their customers. Consequently, every government or business requires an awareness training programme for information security and privacy

(Wlosinski, 2019). Furthermore, Wlosinski (2019) posits that the need for this awareness programme encompasses ethical considerations (especially regarding handling personal information), regulatory mandates, and best practices that help organisations protect themselves from potential threats and unnecessary risks. An awareness programme will significantly contribute to teaching users how to manage information security and privacy in their lives (Beck et al., 2021). This will then positively impact the users, their families, friends, and neighbours.

2.5.7. Critical Success Factors for Security Education Training and Awareness (SETA) Programme

The financial services industry has become increasingly dependent on mobile technology for delivering financial services to users, managing client data, exchanging information, and interacting with customers (Barbu et al., 2021). While mobile phones now provide financial services conveniently, they expose customers to new cyber threats they never anticipated (Makin, 2018). Without adequate protections in place, mobile financial services can pose a risky environment. A report by Myriad Group (2019) indicates that 70% of Kenyans have been victims or know someone who has been a victim of digital financial transaction fraud. The report further reveals that this fraud costs the financial services industry a loss of Kshs five billion ($41.7 million) annually. It demonstrates that the avenues through which customers were targeted for financial service transaction frauds include phone calls (73%), SMS (57%), email (19%), and social media (17%).

As people increasingly rely on mobile technology to access financial services, there must be heightened awareness to change users' behaviours. This effort needs to:

i. Be cultivated by MFS providers in the mobile environment.
ii. Be a continuous endeavour instead of a one-time intervention.
iii. Educate customers about good security habits and the benefits they provide.

The PwC report (2021) on Financial Services Technology 2020 and beyond identifies cybersecurity as one of the top risks for financial institutions. The European Union Agency for Network and Information Security (ENISA) report (2021) lists the top 15 cyber threats, including:

i. Phishing.
ii. Cyberespionage.

iii. Spam.
iv. Data breaches.
v. Malware.
vi. Ransomware.
vii. Insider threat.
viii. Web application attacks.
ix. Botnets.
x. Identity theft.
xi. Physical manipulation/damage/theft/loss.
xii. Cryptojacking.
xiii. Denial of service.
xiv. Web-based attacks.
xv. Information leakage.

It is crucial to note that the human element is central to the success of these attacks. All 15 attacks highlighted in the ENISA report can only be executed successfully with the involvement of the human element, serving as the initiator, agent, or the executor of the respective attack.

Monetary gain motivates the desire for cybercrime (Sutherland, 2016; Wayne, 2022; Peersman et al., 2022). Numerous cybercriminals resort to employing malware to extract funds from customers' bank accounts. Additionally, ransomware has been utilised as another tactic to obtain financial gains from victims. Moreover, cybercriminals may be driven by various motivations, such as curiosity, sabotage, or the desire to cause denial of service (Pawlicka et al., 2021).

Mobile devices and other new technologies have enabled many people to connect to cyberspace, thereby expanding the risks of cybercrime (Ambore et al., 2017). The authors argue that these risks have been further intensified due to the inadequate security practices of mobile device users.

Hackers and cybercriminals exploit human vulnerabilities brazenly, and nobody is immune to information security slip-ups (O'Leary, 2020). The anticipation that mobile device users will bear the ultimate responsibility for securing their devices and safeguarding financial transactions conducted through mobile phones has rendered mobile devices a probable target for cyberattacks (Maurushat & Nguyen, 2022).

From the preceding, it becomes imperative that an effective countermeasure, strong enough to handle the risks created by the human element in perpetuating cybercrime, is necessary. A widely acknowledged saying in the realm of information security is that users constitute the weakest link (Hughes-Lartey et al., 2021; Poehlmann, et al., 2021). While this might be true, awareness programmes should endeavour to make the human element part of the solution rather than the problem. Training and awareness activities should yield the best return on investment.

When implemented appropriately, training and awareness can result in organisations experiencing fewer users falling victim to cyber risks and schemes, such as manipulative social tactics (Tulkarm, 2021).

A good security awareness programme informs users about malicious activity (Susanto, 2021). Therefore, users must be vigilant about typical mobile financial fraud schemes, especially those targeting them (Brecht, 2019). Preparing users to detect phishing or cyber swindles entails that organisations establish policies, procedural instructions, and a comprehensive training system to help identify and report suspicious activities, thus avoiding falling victim to scammers (Brecht, 2019). In any organisation, the human element is both the target and the solution, and no information security tool can compensate for the lack of user awareness (O'Leary, 2020).

The successful implementation of any cybersecurity training and awareness initiative hinges on end-user awareness training. To establish and sustain a successful information security training and awareness initiative, incorporating a variety of "best practices and building blocks" is essential (Subramanian, 2021).

The SP 800-50 (NIST, 2021a) stipulates that training and awareness programmes should be implemented once:

i. A needs assessment has been conducted.
ii. A strategy has been established.
iii. An awareness and training programme plan for realising that strategy has been finalised; and
iv. Awareness and training materials have been developed.

2.6. INFORMATION SECURITY TOPICS AND CONCEPTS

Overcoming cyber threats necessitates that organisations implement measures and programmes ensuring employees and users care for the business by protecting the organisation's data and systems. This study aimed to develop a baseline security awareness and training model for

mobile financial providers and users. The genesis of this study occurred when the researcher observed several security mishaps among mobile financial users. Numerous users lost money from their mobile wallets through means that could have been avoided by increasing their knowledge of information security behaviours. An increase in knowledge is achieved by raising awareness among mobile financial service users.

2.6.1. Research Question #01

As part of this study, the researcher developed research questions to guide the investigation. In this regard, Research Question #01 was as follows:

> **Which information security topics and concepts could form part of the Training, Education and Awareness?**

NIST Special Publication 800-50 (NIST, 2021a) provides recommendations for developing an information security training and awareness programme, creating training materials, and implementing the programme. The NIST Special Publication 800-50 (NIST, 2021a) highlights two primary goals for cybersecurity training and awareness, whereby the developer of the training material should have the following two objectives in mind:

i. What kind of behaviour does the programme intend to emphasise? (Awareness);
ii. What skill(s) does the programme intend the audience to master and practise? (Training).

NIST (2021a) suggests that instruction should include awareness-based educational content and skill development that helps users recognize threats and take appropriate actions to avoid security incidents.

Awareness training is effective in improving information security outcomes only to the extent that it changes users' culture. Comprehensive training is designed to teach users how to identify situations with security risks and how to mitigate those risks (Chowdhury & Gkioulos, 2021). This can be accomplished by allowing users to raise concerns and ask questions about information security. However, this knowledge will only be practiced when users perceive that security is valued in their culture (Larios-Vargas et al., 2022).

With the increasing number of cyber threats and the growing complexity of channels organisations use to deliver services, and connections to systems and data from digital devices, it is becoming increasingly difficult to predict the next accidental leak or threat to the

organisation (Mazzarolo et al., 2021). Information security awareness efforts should enable users to be active protectors of organisations, organisation systems, data, and devices, rather than merely ensuring end-users can choose strong passwords or adhere to specific measures, which could be a form of security theatre (Bhana & Ophoff, 2022).

2.6.2. Security Awareness and Training Topics

The NIST Special Publication 800-50 (NIST, 2021a) proposes that cybersecurity training and awareness should cover the nine topics listed below:

i. Phishing.
ii. Password security.
iii. Removable media.
iv. Safe web browsing.
v. Mobile security.
vi. Social engineering.
vii. Physical security.
viii. Malware.
ix. Working remotely.

Educating and training end users of organisational digital services on cybersecurity best practices have become increasingly important (Daly, 2022). The author posits that, given the increasing sophistication of digital threats and new technologies, the most effective way to prevent security breaches and save organisational time is to educate users on the best cybersecurity practices.

According to an IBM Cyber Security Intelligence Index Report (IBM, 2022b), human error accounts for 95% of cybersecurity breaches. Awareness training sessions can significantly reduce this number (Ahola, 2021). However, studies suggest that only half of all end users receive training once per year, while the other 50% do not receive any form of awareness training (Daly, 2022). The author, therefore, suggests the following 12 topics should form part of cybersecurity awareness training for end users:

i. Physical Security.
ii. Mobile Device Security.
iii. Passwords and Authentication.
iv. Phishing attacks.

v. Removal Media.
vi. Social Engineering.
vii. Public Wi-Fi.
viii. Internet and Email use.
ix. Social media use.
x. Cloud Security.
xi. Working remotely.
xii. Security at home.

The European Union Agency for Cybersecurity, ENISA, published the ENISA Threat Landscape Report (ENISA, 2021). The report highlights information security threats, emerging trends, and current trends. The report is based on data that is publicly available and gives an independent view of threat trends, threat agents, and observed threats. It involves the analysis of reports from networks of excellence, the information security industry, independent institutes, and standardisation bodies. The ENISA (2021) Threat Landscape report highlights 15 top cyber threats and trends that should ideally form part of awareness and training topics for end users. These threats include:

i. Spam.
ii. Identity theft.
iii. Insider threat.
iv. Web-application attacks.
v. Malware.
vi. Denial of Service (DoS).
vii. Web-based attacks.
viii. Physical manipulation, damage, theft, and loss.
ix. Phishing.
x. Ransomware.
xi. Data breaches.
xii. Cryptojacking.
xiii. Botnets.
xiv. Cyberespionage.
xv. Information leakage.

It is essential to note that these core topics on cybersecurity can be further divided into detailed sub-topics. The list provided is an introductory awareness training recommendation for all end users.

2.6.2.1. Phishing

Phishing involves crafting messages to lure recipients and take the bait. It uses social engineering techniques. Phishers aim to lure recipients through email or messages to click on an unsafe website address, open a malicious attachment, send their credentials, or send/wire money. The Cofense Annual State of Phishing Report (Cofense, 2021) shows that phishing attacks have resulted in 91% of successful cyberattacks. These figures undoubtedly demonstrate the need for awareness of phishing attacks. End users should be trained to recognize potentially harmful emails or phone messages and report suspicious ones. Through this, the threat of phishing attacks can be reduced significantly.

2.6.2.2. Password Security

Passwords that are commonly used, simple, or exhibit recognizable patterns can be easily guessed by malicious actors, allowing unauthorised access to users' accounts, or enabling financial transactions on their mobile devices. It is crucial to train users to create randomised passwords that are difficult for malicious actors to decipher. Encouraging users to memorise their passwords instead of writing them down on potentially insecure paper is also important. Implementing two-factor authentication adds an additional layer of security, significantly improving the integrity of users' accounts.

2.6.2.3. Safe Web Browsing

Internet surfing can pose dangers if users do not adhere to secure browsing practices. Training end users to make informed decisions while performing online actions enhances their safety and reduces vulnerability to cyberattacks.

2.6.2.4. Social Engineering

Social engineering is a technique utilised by fraudsters to gain users' trust and subsequently persuade them to divulge sensitive information that can be exploited for fraudulent purposes. This category encompasses several malicious activities, including phishing, baiting, pretexting, and tailgating. The most effective defence involves educating users about the risks and maintaining vigilance.

2.6.2.5. Malware

Malware comprises applications designed to cause damage, disruption, or unauthorised access to computer systems. The ENISA Threat Landscape (ETL) report (2021) identifies this threat as the most prevalent form of attack, accounting for 30% of all data breaches in 2020. According to the same ETL report, mobile device malware was predominantly hosted in third-party application stores, with the highest malware concentrations found in the Lifestyle (27%) and Audio and Music (20%) categories. Mobile banking app malware also saw a 50% increase compared to the 2019 ETL report.

2.6.2.6. Mobile Device Security

As mobile phones increasingly facilitate access to banking systems and financial services, the risk of security breaches correspondingly rises. Educating users about mobile device accountability is essential, as this enables them to avoid risks, password-protect or encrypt sensitive data on their devices and implement biometric authentication to safeguard information in case of theft or loss.

2.6.2.7. Physical Security

Given that many attacks occur through digital means, ensuring the physical security of mobile devices, sensitive documents, and passwords is crucial to minimise information security risks. Users require training on the dangers of leaving sensitive items unattended. The ENISA (2021) Threat Landscape report indicates that 25% of data breaches in the financial sector resulted from mobile device theft or loss, contributing significantly to data leakages. Additionally, 46% of businesses feel vulnerable due to potential risks associated with losing mobile devices.

2.6.2.8. Removal Media

Removable media, such as portable devices used for transferring files between computers, can be exploited by attackers. By using USB devices containing malware, users may inadvertently run malicious software that compromises their data and device integrity. Training mobile device users to handle removable media safely and responsibly is crucial.

2.6.2.9. Working Remotely

As an increasing number of organisations permit staff to work remotely or users to access financial services offsite, it becomes essential to educate them on secure working practices. The growing trend of remote work heightens the threat of security breaches, especially when users lack training on the risks associated with working remotely. Mobile devices should be

configured to lock automatically after a period of inactivity and be equipped with antivirus software.

2.6.2.10. Public Wi-Fi

Users may occasionally access financial systems and services while traveling. In such instances, the only available internet access might be through public Wi-Fi. Consequently, it is crucial to educate users on the safe use of public Wi-Fi. This is necessary because some fake public Wi-Fi networks, masquerading as free Wi-Fi in malls, restaurants, and coffee shops, may expose users to vulnerabilities as they enter sensitive information through non-secure networks. Training users on how to use public Wi-Fi safely and educating them about the signs to watch for in identifying frauds can enhance awareness and effectively assist in managing such risks.

2.6.2.11. Cloud Security

Cloud services have transformed the way organisations store and access data. With much private data stored in remote locations, the risk of large-scale hacks is significant. As organisations focus on data protection, selecting the right cloud service provider is essential to ensure a secure and cost-effective means of storing organisational data. A study by Gartner (2019) revealed that 99% of all cloud security incidents resulted from end-user errors. It is thus vital to include training and guidance for users on the safe and secure use of cloud-based solutions and applications as part of cybersecurity awareness efforts.

2.6.2.12. Social Media Use

Many individuals routinely share significant aspects of their lives on social media, including holidays, events, and work-related matters. Users should be encouraged to exercise caution and restraint when sharing information online, as oversharing can lead to sensitive information being exposed on social media platforms. This may allow malicious actors to impersonate trusted individuals. Training users to set privacy settings on their social media accounts is essential. By educating staff and customers, organisations can help mitigate the risk of potential advantages that cybercriminals might otherwise gain from connections to organisational networks or attempts to trick customers into divulging sensitive financial and other types of information.

2.6.2.13. Internet and E-Mail Use

Based upon findings from a 2018 poll, it was revealed that approximately 59% of end-users have the habit of employing identical passwords for multiple accounts (Truta, 2018). This means that an individual might use the same password for Yahoo, Hotmail, Gmail accounts, and even their banking applications. Consequently, if one account is compromised, a hacker could potentially access all of a user's accounts. Many websites also offer free software downloads that may be infected with malware. As such, users must be trained to download software from trusted sources, which is the only guarantee against installing malicious software. Training employees and users on safe internet habits is the most effective defence against such threats.

2.6.2.14. Security at Home

As people can continue working with organisational data using personal devices from home, it is necessary to manage the associated risks. Malware applications inadvertently downloaded on personal devices can compromise the organisation's network if login details are obtained. This is because malicious actors do not limit their attacks to the workplace alone. Therefore, users should be trained to maintain safe internet use at home.

2.6.2.15. Spam

This type of cyber threat involves the use of abusive and unsolicited emails and messages that inundate recipients' accounts. Part of user training to safeguard against spammers should involve asking questions such as: who sent this message or email; is it safe to open this email attachment; is the email or message content and subject familiar and sensible? among others.

2.6.2.16. Data Breaches

A data breach refers to an incident wherein information is illicitly obtained from a system without the awareness or authorisation of the system's owner. Data that may be stolen includes sensitive, confidential, or proprietary information, such as an organisation's customer data, credit card numbers, or matters relating to a country's national security. The ENISA Threat Landscape (2021) report reveals that 71% of data breaches reported were financially motivated. The same report indicates that over 25 million records were exposed or compromised each day in the first half of 2020. The United States of America (USA) alone reported 22 million records stolen up to July 2020. Consequently, organisations should implement security awareness

programmes to train employees and users in identifying and reporting suspicious emails or messages.

2.6.2.17. Insider Threat

An insider threat refers to the intentional or unintentional abuse of access to an organisation's digital data by current or former employees, partners, or contractors. The three common insider threat types are:

i. The negligent insider – does not follow security policies and instructions regarding information security.
ii. Malicious insider – acts deliberately.
iii. Compromised insider – acts accidentally as an agent of the malicious attacker.

Users should be trained on their role in the information security chain and how not to fall prey to attackers (Chidukwani et al., 2022).

2.6.2.18. Information Leakage

Information leakage involves the disclosure of sensitive data processed and stored by an application. Consequently, information is unintentionally disclosed, potentially aiding attackers in their efforts to breach application security. The compromised information could be personal data or organisational data stored in IT systems. Information leakage can result from an individual's action, process failure in an organisation, technical error, or system misconfiguration. As part of mitigation strategies, it is essential to regularly educate and train an organisation's end users.

2.6.2.19. Identity Theft

Identity theft encompasses fraudulent activities that occur because of stealing personally identifiable information, exploiting the widespread digitisation of personal data. This nefarious practice entails intentionally assuming another individual's identity to obtain financial gain, credit, or other advantages in the victim's name. Generally, the individual whose identity has been stolen suffers adverse consequences. Protection against identity theft requires regular training of users on protecting sensitive information, ensuring that they do not disclose such information to unsolicited recipients via email, phone, or in person.

2.6.2.20. Ransomware

This denotes the malevolent utilisation of software designed to restrict access to a computer system, digital device, or specific files, with the intent of extorting a ransom from the affected

party in exchange for restoring access. Most ransomware variants encrypt the files on the target device, rendering them inaccessible, and demand payment before access can be restored. Therefore, organisations must invest in user awareness to promote secure browsing behaviour.

2.7. EFFECTIVE SECURITY AWARENESS PROGRAMME

Hudgens (2017) presents 10 elements that constitute an effective security awareness programme. While these elements apply to employees within an organisation, they are also relevant to users with access to organisational systems enabled by Mobile Financial Services. The importance that organisations place on employees regarding information systems security training and awareness should be extended to users who can access these systems using mobile devices that the organisation does not manage since "outsiders" have now become "insiders," thus increasing the information security risks. These elements include:

2.7.1. Leadership

Senior leadership plays a critical role in awareness and training activities and programmes. They provide and approve funding for training and awareness initiatives. The tone for the programme and support for the message regarding the significance of information security in accomplishing business goals and objectives are set by the involvement of leadership. The significance attached to awareness and training programmes, as well as the organisation's commitment to information security programmes, is demonstrated by the engagement of leadership.

The successful launch of an Information Security Education, Training, and Awareness (SETA) programme necessitates significant investment planning to ensure that adequate funding is allocated to cover the requirements of the awareness and training programme. The budget should support cybersecurity awareness training plans, meeting the costs of any contracts, and learning materials that are prepared and supplied by trainers (Brecht, 2019). Therefore, from the outset, there is a need to develop a long-term plan with clear options funded through senior management's support (Brecht, 2019). Funding and budgetary allocations for information security awareness initiatives can only be achieved if there is evidence of support from leadership. The leadership should provide funding for bulk SMS, security and awareness IT infrastructure, and the printing of security and awareness brochures and flyers, among other things. Leadership involvement in security and awareness initiatives ensures accountability

for the programme's success or failure. Such visible support will significantly contribute to the success of information security awareness programmes.

2.7.2. Learning

Users of Mobile Financial Services come from diverse age groups, and each age group learns differently. Users have different interests and learning styles, and specific ways of conveying information may already be saturated (Brecht, 2019). Therefore, it is crucial to consider awareness and training activities that accommodate different generations of learners to ensure content retention. Similarly, mobile financial services users come from diverse academic backgrounds, with some having no education. Instruction designers need to be creative in devising ways to reach all users. The instruction designer can use a mix of emails (for those with formal education), SMS alerts, roadshows, or periodic town hall meetings based on the target audience's profile. This approach will ensure that information reaches all users and prevent complacency and monotony.

Additionally, any awareness and training proven to be effective in the organisation's situation can be delivered in various ways, ranging from seminar-style group demonstrations to practical classroom-style or instructor-led training (Brecht, 2019).

2.7.3. Strategy

An effective SETA programme requires a long-term strategy that reflects the leadership's vision for the security culture they hope to instil in mobile financial services users. This strategy will be supported by a two-year plan that details quarterly information security topics and themes that must be developed. Awareness training activities will then be focused on these topics and themes. The strategy will also define any timelines for introducing the information security programme and state the objectives and scope of the awareness training. If there is no clear strategy, the awareness initiatives will fail.

2.7.4. Analytics

A proper balance of activities and information necessitates the establishment of metrics. Initially, a baseline should be designed to comprehend users' current information security culture. Following the establishment of this baseline, it becomes imperative to devise appropriate metrics that can effectively facilitate data collection and analysis. The primary goal is to determine whether the users' security culture is progressing in alignment with the desired direction, as articulated in the strategy. These metrics can refine and demonstrate the

training and awareness programme's success. Progress measurement is vital to determine if information security training and awareness needs are adequately addressed or if there is a lack of improvement in a specific area. Effective information security metrics can identify weaknesses, establish trends for improved information security resource utilisation, and gauge the failure or success of information security awareness initiatives implemented by the organisation (Brecht, 2019).

2.7.5. Persistence

Careful consideration should be given to the frequency of awareness and training sessions (Brecht, 2019). The cultivation of cybersecurity awareness should be viewed as an ongoing process, rather than a singular event. Annual information security awareness training sessions are insufficient. To achieve greater persistence, it is essential to schedule training and awareness sessions throughout the year. As cyber risks continually change and new threats emerge, training and awareness programmes must be responsive enough to provide information on emerging threats and their countermeasures. Instruction designers should thoughtfully plan the persistence of information security messages for users. Mobile financial service providers should consistently and persistently send SMS messages, emails, hold town hall meetings, or organise roadshows to inform users about emerging threats. If the message is persistent and consistent, users may be reminded when confronted with a cybersecurity threat.

2.7.6. Timeliness

Information must be promptly provided to users, reflecting the latest news about cyber threats. Organisations must remain vigilant, stay ahead of cybercriminals, and inform their mobile financial services users about emerging threats and how to counter such attacks. Timely information can help prevent cyber-attacks or users falling victim to attacks that could result in significant financial loss.

2.7.7. Relevance

Training and awareness activities should include guidance on users' interactions with mobile financial services, the devices they use to access these services, and the risks involved when allowing someone to access or perform services on their behalf. The training and awareness programme must address the risks and necessary precautions for users. It is crucial for everyone to take an active role in information security, thus reducing exposure to cyber threats.

2.7.8. Feedback

Requesting ideas from end users or encouraging them to provide feedback on awareness training sessions is good practice. A mechanism for obtaining user feedback on performance after awareness training sessions is essential. This feedback allows instruction designers to evaluate the growth and success of the awareness training programme (Lohrmann, 2014). Trainers should listen to ideas, suggestions, and issues users encounter during awareness training. If one person speaks up, it is likely that several others are experiencing the same issues without speaking up.

One method of obtaining feedback is by sending users simulated social engineering tactics used in successful attacks on individuals. The responses received from users can indicate whether additional training is necessary or if they understood the training content.

2.7.9. Incentives

Users appreciate incentives, which can be incorporated into the awareness and training programme. Mobile financial providers can offer merchandise, such as caps and pens, as incentives. This approach may encourage other users to attend when they hear about a security and awareness training session organised by a Mobile Financial Service provider in their area. It can significantly increase the number of users trained on emerging cyber threats and how to counter such attacks.

Awareness training for MFS users should become an integral part of organisations providing Mobile Financial Services. An effective security awareness programme ensures that users are well-equipped to identify, avoid, or counter information security incidents (Lohrmann, 2014). It is essential to understand that a successful information SETA programme has a continuous life cycle and must be consistently evaluated for improvement. This evaluation contributes to increased usability and sustainability; otherwise, inconsistent efforts could expose users and organisations to heightened risk (Brecht, 2019; NIST, 2014; Chaudhary et al., 2022).

2.8. SECURITY EDUCATION TRAINING AND AWARENESS (SETA) GOALS AND OBJECTIVES

The goal of a SETA programme is to drive positive behaviour change that supports cybersecurity objectives (Alshaikh et al., 2021). The primary objective of a SETA programme is to foster a comprehensive understanding among users regarding their responsibility in safeguarding the Confidentiality, Integrity, and Availability (CIA) of information and

information assets. It is imperative to acknowledge that cybersecurity is a collective endeavour, extending beyond the confines of the cybersecurity department. This recognition underscores the significance of every individual's role in upholding cybersecurity measures (Yusif & Hafeez-Baig, 2021). It is essential for users to grasp the significance of safeguarding information, moving beyond a mere understanding of how to protect an organisation's data.

Previous cybersecurity awareness programmes have not succeeded in altering users' attitudes toward recognising, blocking, or reporting cyber threats. Consequently, users' actions and errors continually expose their status as the vulnerability in cybersecurity (Sabillon, 2022). The perception that humans represent the point of susceptibility in the security chain arises from inadequate training and unawareness regarding cybersecurity. Alshaikh et al. (2021) contend that current SETA initiatives primarily increase users' knowledge acquisition, rather than altering behaviour and beliefs. Users ought to understand how their actions can significantly impact an organisation's security posture (Krutz & Russell, 2001; Aldawood & Skinner, 2019). Therefore, a SETA programme should aim to reinforce information security policies and practices endorsed by the organisation (Hu et al., 2022). Wood (1999) asserts that SETA contributes to accelerating new software systems development, reducing the cost of security incidents, and ensuring the uniform application of controls across an organisation's IT systems.

A fundamental awareness programme for customers regarding security should address issues such as the importance of passwords, the structure of strong passwords, setting devices to lock after periods of inactivity, the significance of updating the phone's operating system and applications, the risks associated with jailbroken devices, and the implementation of antivirus and encryption whenever possible (Pegueros, 2013; Madhav & Tyagi, 2022). Furthermore, if a carrier supports remote wiping, users should enable the capability to remotely wipe their devices in case of loss or theft.

Enhancing cybersecurity awareness stands as a pivotal element in safeguarding organisations against potential attacks (Grassegger & Nedbal, 2021). Security awareness programmes will not succeed unless they are designed to change users' attitudes toward cybersecurity (Sabillon, 2022).

2.9. MOBILE SECURITY EDUCATION, TRAINING AND AWARENESS (SETA) IN KENYA

Mobile phones serve an indispensable role in enhancing the provision and accessibility of financial services in Kenya. The greatest beneficiaries of financial services worldwide include rural populations and low-income earners with limited or no access to banks. Mobile penetration and access to financial services have led to significant adoption of MFS, particularly among these two groups in developing nations where bank penetration is limited. In developing countries, a considerable segment of the population faces limited access to traditional banking services, mainly because of infrastructure limitations and lower literacy rates (Victor, 2014; Haider, 2018; Feyen et al., 2021). Traditional banking service delivery allowed banks to conduct due diligence before a transaction. This is not possible with MFS, where customers can perform transactions anytime and anywhere.

The growth of MFS has prompted banks in Kenya to adopt the provision of financial services through digital devices. For instance, in its third-quarter 2019 financial report, Equity Bank (2020) revealed that it had recorded Kshs 9.1 billion (US$75.8 million) worth of transactions through its Easy-pay mobile financial service in the first nine months of the year. James Mwangi, the CEO of Equity Group, stated that 93% of transactions were conducted on mobile devices, and the lender was focusing more intently on providing digital payments. This trend in Kenya is evident among all banks, with each advocating for the provision of financial services through digital channels.

This shift towards offering financial services via digital channels has introduced another security requirement for banks to protect customer funds. The growth of MFS has led to an increase in cyberattacks on this financial service delivery channel both in Kenya and globally (Afriyie & Sambasivam, 2023; Salo-Lahti, 2022). The Communications Authority of Kenya (2021) reported a 37.27% increase in cyberattacks from 28 247 819 incidents to 38 776 699 incidents over three months in its April-June report. The report further indicated that threat actors targeted unsecured mobile devices by spreading Trojan apps disguised as legitimate apps in official app stores, such as layout themes, phone utility apps, and popular games. These apps are then used to spread malware or spyware that can infiltrate networks, steal data, and infect devices.

Kaspersky, a leading cybersecurity firm, reported in its 2020 Lab reports (Kaspersky, 2021) that Kenyan users accounted for one in four of the two million attacks reported in Africa in

2020. The report showed that Kenya recorded half a million attacks, second only to South Africa, which experienced 616,616 phishing and spam attacks. Kaspersky's (2022) mobile threats report indicated that 46 million mobile users were attacked. Kenya ranked third in Africa for malware attacks blocked by Kaspersky from January to June 2021. Cisco's (2021) threat reports showed that the largest portion of attacks on mobile users came from malware at 80.69%. An essential observation is that the risk factor escalates significantly when one uses the same phone to access social media platforms, corporate data, and financial services.

In 2017, Jefwa reported that ESET, a reputable cybersecurity company, unveiled a commendable initiative offering complimentary online cybersecurity training to firms in Kenya (Jefwa, 2017). This awareness training was specifically designed to empower businesses in the country to effectively mitigate the repercussions of cyberattacks and data breaches, which have emerged as an escalating global threat to business operations. In May 2017, ESET conducted a survey across its North American markets and discovered that over 30% of respondents had never received any form of cyber awareness training in their workplaces, even though numerous cyber breaches are attributed to employee errors and omissions (ESET, 2017). This finding highlights the critical need for businesses to invest in cybersecurity training programmes to bolster their defence against potential cyber threats stemming from within their organisations. The ESET Cybersecurity Awareness Training modules encompass various essential topics, such as recognising phishing emails, web and email protection, password best practices, social engineering, two-factor authentication, and Internet of Things (IoT) security. Through the provision of these training modules, ESET aims to equip individuals and businesses with the requisite knowledge and skills to actively defend against cyber threats, thereby enhancing their overall cybersecurity resilience.

Most security incidents result from negligence or unaware users (Bharati & Suguna, 2014; Yeo & Banfield, 2022). Despite these challenges, neither banks nor Mobile Network Operators have made a deliberate effort to develop structured ways of conducting SETA. It is essential to note that such a guideline on SETA should consider users' different economic and geographic backgrounds and education levels. Research conducted in Tanzania reveals a direct correlation between the level of cybersecurity awareness among mobile banking users and their education level. Particularly, individuals in the 25–36 age group exhibit higher levels of awareness compared to other demographic groups. This finding suggests that higher education levels in this age bracket might contribute to a greater understanding of cybersecurity risks and

the importance of adopting safe practices while engaging in mobile banking activities (Malero, 2015; Fatokun et al., 2019).

The government of Kenya should consider introducing cybersecurity education and training in the school curriculum. Organisations need to establish structured ways of carrying out cybersecurity training and awareness at the enterprise level (Bett, 2020). In response to the growing cyber threats in the financial services industry, Kenya's Central Bank issued guidance on cybersecurity for financial service providers in August 2017 (CBK, 2017). The guideline requires institutions to:

i. Implement training and awareness programmes on IT security to provide information on common threat types, best practices for IT security, and procedures and policies for each institution. This training should target boards, senior management, and all other employees.
ii. Establish a standardised plan to provide technical training to cybersecurity specialists in the organisation on an ongoing basis.
iii. Ensure that customers, partners, service providers, or any third party with access to the bank's IT infrastructure receive awareness and information on cybersecurity.

The guideline requires financial institutions to inform the Central Bank of Kenya within 24 hours about any cybersecurity incidents that can significantly and adversely affect the institution's ability to provide services to its customers, reputation, or financial position. Although this is a significant step in the fight against cybersecurity, it does not specify how this should be achieved. Perhaps this is why there has been a continuous rise in cyber threat incidents since its publication in 2019, rather than a reduction in numbers.

Despite Kenya being a giant in Africa and the world in mobile money services (McBride & Liyala, 2021; Mpofu, 2022), there is little progress in higher education institutions to prepare cybersecurity specialists to address the increasing cybersecurity threat. A closer look at educational institutions paints a grim picture. Out of the 34 public and 33 private universities accredited by the Commission for University Education, only four offer programmes in Information Security, and none offer courses on Mobile Security or Mobile Information Security. The other institutions merely provide training for information security certifications from professional bodies. The information security-related courses offered are presented in Table 2.9.

Table 2.9 Security Courses in Institutions

Course	University	Degree type	Duration
Information System Security	Strathmore	Masters	2 years
PhD in Information Security & Audit	Jaramogi Oginga Odinga University of Science and Technology	Doctoral	4 years
Master of Science in Information Technology Security and Audit	Jaramogi Oginga Odinga University of Science and Technology	Masters	2 years
Postgraduate Diploma in Information Technology Security	Jaramogi Oginga Odinga University of Science and Technology	Postgraduate Diploma	
Master of Science in information technology management	University of Nairobi	A one-semester module on Information Systems Security and Audit	16 weeks semester
Master of Science in Information Security (Cyber Crime)	Mount Kenya University	Masters	2 Years
Cyber Security	Strathmore(iLab)	Masters	2 years
Certified Ethical Hacking (CEH)	Strathmore Computer pride	Professional Certification	6 months
Certified Ethical Hacking (CEH)	Riara	Diploma	2 years
Certified Information System Auditor (CISA)	JKUAT Computer pride	Professional Certification	4 months
Information security and Forensics	KCA	Bachelor	3 years (tri-semesters)
Information Security and Ethical hacking	Institute of Software Technologies	Diploma	1 year

Source: Compiled by the Researcher[2]

[2] Prepared by consolidating data from different university websites.

It is crucial for policymakers to be proactive in developing a curriculum to train individuals, both current and future employees, as outlined in the CBK guideline for cybersecurity for financial institutions (CBK, 2017).

2.10. CHAPTER SUMMARY

The rise of Mobile Banking Services has significantly expanded opportunities, especially for the unbanked and rural populations, including the chance to attain financial inclusion previously unavailable to them. They can now receive money conveniently. Through MFS, banking services are now conveniently available to users, allowing them to access them from the comfort of their offices or homes, eliminating the necessity of visiting a physical banking hall. However, this channel has also introduced numerous cybersecurity challenges for both MFS providers and users. These cybersecurity challenges can be mitigated with appropriate Security Education Training and Awareness (SETA) measures and strategies.

This chapter has presented the concept of an IT system as a background before critically examining developments in Mobile Financial Services and its Adoption, Security and Privacy in MFS, Security theatre and its impact on effective security, Critical Success Factors for an effective SETA programme, and the state of Information Security Education, Training, and Awareness in Kenya.

By understanding the importance of SETA and incorporating it into the educational system and workplace training, Kenya can better address the growing cybersecurity threats related to mobile financial services. Policymakers should collaborate with educational institutions, industry professionals, and financial service providers to develop comprehensive and targeted SETA programmes. These programmes should be created to address the unique requirements of different groups of users, considering their varying economic, geographic, and educational backgrounds.

In conclusion, the rise of mobile banking services in Kenya has brought both opportunities and challenges. To maximise the benefits and minimise the risks, it is vital to invest in cybersecurity education, training, and awareness for all stakeholders, from employees and management to customers and service providers.

Chapter 3: Theoretical Frameworks

Every theory is a self-fulfilling prophecy that orders experience into the framework it provides.

Ruth Hubbard

3.1. INTRODUCTION

Mobile financial services (MFS) have revolutionized the financial industry, offering unparalleled convenience and accessibility. However, this evolution has also introduced new cybersecurity challenges. MFS users are frequently targeted by cybercriminals due to the sensitive nature of financial data. Effective cybersecurity awareness and training initiatives are critical in mitigating these risks associated with mobile financial transactions. Cybersecurity frameworks offer structured approaches to manage and mitigate risks. In this chapter, a further review of literature is conducted in chapter. The literature review conducted in this section relates to cybersecurity theories with a view to developing a new model This section examines the NIST Cybersecurity Framework, Cybersecurity Awareness Training Model (CATRAM), and the MediaPro Adaptive Awareness Framework, highlighting their strengths and applicability in developing a cybersecurity awareness model for training and awareness initiatives for users of mobile financial services. The model serves as a lens through which the researcher views the role of awareness in improving secure behaviour among users of mobile financial services. Similarly, the research objectives, research questions, theoretical framework and the research instruments are aligned to provide a coherent strategy with which the research questions are addressed as shown on table 3.2.

3.2. THE NIST CYBERSECURITY FRAMEWORK

3.2.1. Overview

The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology, is a comprehensive guideline designed to help organizations manage and reduce cybersecurity risk. The framework is designed to help organisations understand and evaluate cybersecurity threats, prioritize opportunities for improving the management of risk, and establishing a common language for communicating about cybersecurity needs, concerns, expectations, and capabilities (Impact, 2024). It consists of five core functions: Identify, Protect, Detect, Respond, and Recover. These functions are further divided into categories and

subcategories, providing a structured approach to cybersecurity management (NIST, 2018). Recently, a sixth function, Govern, has been introduced to emphasize the importance of governance in cybersecurity practices (NIST, 2020; NIST, 2023).

3.2.2. Components

The NIST cybersecurity framework has six components (NIST, 2018).

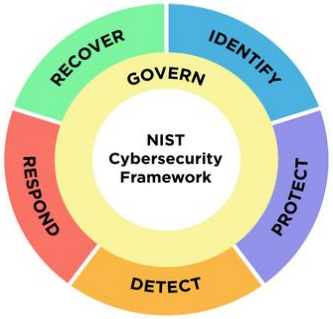


Figure 3.1 NIST Cybersecurity Framework

Source: https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0

Identify: This function involves understanding the organization's cybersecurity risks, including asset management, business environment, governance, risk assessment, and risk management strategy.

Application of this component to Mobile Financial Services:

User Education: Involves educating users about the types of personal information and financial data stored on their mobile devices.

Risk Awareness: Involves making users aware of the potential threats, such as phishing, malware, and unauthorized access, that can compromise their financial information.

Asset Management: Involves encouraging users to maintain an inventory of their devices and understand the importance of securing each device used for financial transactions.

Protect: This function focuses on safeguarding critical infrastructure and information through access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology.

Application of this component to Mobile Financial Services:

Authentication and Authorization: Train users on the importance of strong passwords, biometric authentication, and multi-factor authentication (MFA) for accessing financial apps.

Software Updates: Emphasize the need for regular updates to mobile operating systems and financial applications to patch security vulnerabilities.

Data Protection: Educate users on encrypting sensitive data and using secure connections (e.g., avoiding public Wi-Fi for financial transactions).

Detect: This function encompasses activities to identify the occurrence of a cybersecurity event, including anomalies and events, security continuous monitoring, and detection processes.

Application of this component to Mobile Financial Services:

Anomalous Activity: Involves teaching users to recognize unusual activities on their accounts, such as unexpected transactions or login attempts from unfamiliar devices.

Notification Settings: Encourage users to set up alerts and notifications for their financial accounts to detect suspicious activities promptly.

Monitoring Tools: Involves informing users about mobile security apps that can help detect and alert them to potential threats.

Respond: This function involves taking action after a cybersecurity event, including response planning, communications, analysis, mitigation, and improvements.

Application of this component to Mobile Financial Services:

Incident Reporting: This involves educating users on how to report suspicious activities to their financial service providers promptly.

Response Plans: Provide guidelines on immediate steps to take if a device is lost or stolen, such as remotely wiping data and notifying their financial service provider or security agencies.

Containment and Mitigation: Instruct users on isolating their compromised device from other networks and services until it is secured.

Recover: This function focuses on restoring services and capabilities after a cybersecurity incident, involving recovery planning, improvements, and communications.

Application of this component to Mobile Financial Services:

Backup and Restore: Stress the importance of regularly backing up financial data and how to restore it after a security incident.

Continuous Improvement: Encourage users to review and update their security practices regularly, learning from past incidents to enhance their security posture.

Support Resources: Inform users about resources available from their financial service providers, such as customer support and fraud resolution services.

Govern: This function emphasizes establishing and maintaining a governance structure that sets the direction for cybersecurity and privacy efforts. This function involves establishing oversight and ensuring that cybersecurity activities align with organizational objectives. This newly added function highlights the necessity of governance in cybersecurity, emphasizing risk management, policy development, and organizational structure alignment (NIST, 2022).

3.2.3. Suitability for Mobile Financial Services

The NIST Framework's structured approach provides a solid foundation for developing comprehensive cybersecurity awareness programs. Its emphasis on risk assessment and training aligns well with the needs of MFS users, who must be aware of the specific risks associated with mobile transactions. The detailed guidelines for protection and detection also help in creating effective training modules that address real-world scenarios relevant to MFS. Additionally, its structured methodology provides a robust foundation for identifying and mitigating risks specific to mobile financial services. The "govern" function ensures that cybersecurity efforts align with the organization's objectives, which is critical for financial services organizations that handle sensitive data (NIST, 2023). This alignment is critical for mobile financial services, where regulatory compliance and risk management are paramount. By implementing the NIST framework, mobile financial services can develop robust cybersecurity policies, continuously monitor threats, and respond effectively to incidents, ensuring the protection of sensitive financial data (NIST, 2022). The framework's adaptability allows it to be customized to address specific challenges in the mobile financial services sector.

3.3. THE CYBERSECURITY AWARENESS TRAINING MODEL (CATRAM)

CATRAM was originally conceived to deliver awareness training for the members of the Board of Directors, Top Executives, Managers, IT (Information Technology) staff and of course, end-users (Sabilion et al., 2019). This model emphasizes the importance of continuous education

and training to enhance users' cybersecurity awareness since cybersecurity awareness plays an important role in the human arena of cybersecurity. CATRAM is designed to improve the cybersecurity awareness and behaviour of individuals within organizations. The model integrates various training and awareness activities to enhance users' understanding of cybersecurity threats and best practices (Sabilion et al., 2019). CATRAM focuses on enhancing individual awareness and behaviour towards cybersecurity threats. It emphasizes structured training and continuous education, tailored to the specific needs and knowledge levels of users (Arachchilage & Love, 2014).

3.3.1. Components

Awareness Campaigns: These are designed to increase the general awareness of cybersecurity threats among users. It involves informing users about potential cybersecurity threats and best practises. Within Mobile Financial Services (MFS), it will involve educating users about specific threats to MFS, such as phishing attacks, SIM swapping, malware, and fraudulent apps. Training content would then include how users can identify phishing messages and suspicious links, importance of downloading apps from trusted sources and how to recognize signs of a compromised account.

Training Programs on Behavioural Changes: Structured training sessions that educate users on specific cybersecurity practices and procedures. This section is concerned with encouraging users to adopt secure behaviours when using mobile devices for financial transactions. Within the MFS ecosystem, it will involve training users on how to set up strong, unique passwords and biometric authentication. Users will be trained on how to regularly update the apps and the mobile device operating system, avoiding the use of public Wi-Fi to perform financial transaction and using a VPN when necessary. Users should also be trained on how to enable two-factor authentication (2FA), using apps permissions wisely and knowing which data they are sharing in addition to using inbuilt security features like remote swipe and device encryption.

Simulation Exercises: These involve practical exercises such as phishing simulations to test and improve users' response to potential threats.

Assessment and Feedback: Regular assessments to measure the effectiveness of the training and provide feedback for improvement. Within the MFS ecosystem, it involves collecting feedback from users to assess the effectiveness of the training and identify areas for

improvement. It's important to use metrics such as quiz scores, completion rates, and incident reports to measure the impact of the training. Additionally, its vital to regularly update the training content to address new threats and incorporate user feedback. This component will also involve establishing a cycle of ongoing education, ensuring users stay informed about the latest security practices.

3.3.2. Suitability for Mobile Financial Services

While CATRAM is effective in promoting awareness and changing user behaviour, it lacks the comprehensive structure provided by NIST, making it less suitable for large-scale implementation in mobile financial services. Additionally, CATRAM does not align well with comprehensive risk management strategies or compliance requirements. Similarly, CATRAM lacks the depth needed to address specific regulatory standards or complex risk landscapes.

3.4. MEDIAPRO ADAPTIVE FRAMEWORK

The MediaPro Adaptive Awareness Framework is designed to create a culture of security through adaptive learning and continuous improvement. It leverages data analytics to customize training based on user behaviour and risk profiles (MediaPro, 2018). The MediaPro Adaptive Awareness Framework is a dynamic approach to cybersecurity training that focuses on tailoring training programs to the needs and behaviours of individual users. This framework emphasizes adaptive learning, which adjusts training content based on the user's knowledge level and risk profile (MediaPro, 2020).

3.4.1. Components

The Adaptive Awareness Framework designed by MediaPro offers organisations a measurable and actionable way to introduce better security awareness into organizations. The Framework is designed to adapt to all of an organisation's awareness needs rather than taking a one-size-fits-all approach (8Pillars, 2018). It is a flexible and self-correcting model that encourages organisations to assess their risks, develop a plan for improvement, and provide training and reinforcement (8Pillars, 2018).

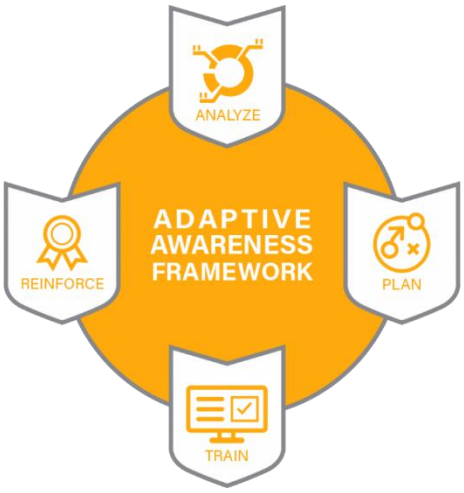


Figure 3.2 MediaPro Adaptive Awareness Framework

Source: https://www.8pillars.com.au/products/mediapro/

Analyse: This initial phase involves evaluating the current security awareness levels of users through surveys, quizzes, and simulated phishing attacks. This process involves identifying risk profiles and knowledge gaps through data analytics. The Analyse component involves assessing the current state of awareness and identifying the specific risks and vulnerabilities that need to be addressed. This step is critical for understanding the unique security challenges faced by users of mobile financial services.

Application to Mobile Financial Services:

Risk Assessment: Evaluate the specific threats to mobile financial services, such as phishing, malware, and unauthorized access.

User Behaviour Analysis: Understand how users interact with mobile financial services, including common mistakes and risky behaviours.

Identify Gaps: Determine the current level of awareness and pinpoint areas where users lack knowledge or exhibit unsafe practices.

By thoroughly analysing the security landscape and user behaviour, organizations can tailor their awareness programs to address the most pertinent risks. For mobile financial services, this might include focusing on educating users about secure login practices, recognizing phishing attempts, and safeguarding their personal information.

Plan: Planning involves designing a strategic approach to address the identified risks and gaps in awareness. This step includes setting objectives, developing content, and deciding on the delivery methods.

Application to Mobile Financial Services:

Objective Setting: Define clear goals for the awareness program, such as reducing incidents of fraud or increasing user knowledge about secure transactions.

Content Development: Create relevant and engaging content that addresses the specific security issues identified during the analysis phase. For mobile financial services, this could include tutorials on enabling two-factor authentication, recognizing fake apps, and avoiding public Wi-Fi for transactions.

Delivery Methods: Choose the most effective channels to reach users, such as in-app notifications, SMS alerts, emails, and interactive tutorials within the mobile app.

A well-thought-out plan ensures that the awareness program is focused and effective. By aligning the content and delivery methods with the habits and preferences of mobile financial service users, organizations can maximize the impact of their awareness efforts.

Train: Training involves executing the planned awareness activities and educating users about security best practices. This step is where users are actively engaged in learning. This component is concerned about getting the right content to the right people at the right time.

Application to Mobile Financial Services:

Interactive Training: Offer engaging training sessions, such as in-app interactive tutorials, webinars, and simulations that demonstrate potential security threats and how to avoid them.

Gamification: Use gamified elements to make learning about security fun and engaging, encouraging users to participate more actively.

Scenario-Based Learning: Provide real-life scenarios that users of mobile financial services might encounter, helping them understand the practical application of security measures

Effective training ensures that users not only receive information but also understand and remember it. For mobile financial services, this means users will be better equipped to recognize and respond to security threats, ultimately reducing the likelihood of security incidents.

Reinforce: Reinforcement involves continuously reinforcing the security messages and practices learned during training. This step helps to ensure that security awareness becomes

ingrained in users' daily habits. This component is concerned with implementing techniques to keep users engaged and reinforce learned behaviours.

Application to Mobile Financial Services:

Regular Updates: Send regular reminders and updates about security best practices through in-app messages, emails, and push notifications.

Continuous Engagement: Keep users engaged with ongoing challenges, quizzes, and refreshers that reinforce key security concepts.

Feedback Mechanisms: Provide users with feedback on their security behaviours, such as alerts when risky actions are detected, and encourage improvements.

Reinforcement helps to maintain a high level of security awareness over time. For users of mobile financial services, continuous engagement and reminders are essential to keeping security at the forefront of their minds, thereby reducing the risk of lapses in secure behaviour.

3.4.2. Suitability for Mobile Financial Services

The adaptive nature of the MediaPro Framework makes it particularly suited for MFS cybersecurity awareness. This adaptive approach ensures that training is relevant and engaging, enhancing its effectiveness in changing user behaviour and reducing cybersecurity risks. Its focus on personalized training and continuous reinforcement ensures that users remain vigilant against new and evolving threats. By regularly assessing and updating training content, this framework can effectively address the dynamic threat landscape of mobile financial services. The MediaPro Framework's emphasis on human behaviour and adaptive learning aligns well with the need for user-centric cybersecurity awareness programs. Its personalized training modules ensure that users are engaged and informed about relevant threats. Similarly, the MediaPro Framework's adaptability and continuous learning cycle make it inherently suitable for the rapidly changing MFS environment. Mobile financial services often involve a diverse user base with varying levels of cybersecurity knowledge. The adaptive learning approach ensures that each user receives training that is relevant to their specific needs and risk profile. This personalized approach enhances the overall effectiveness of the training program, leading to better user engagement and improved cybersecurity practices.

3.5. PROPOSED INTERGRATED AWARENESS MODEL

Combining the constructs from the NIST Cybersecurity Framework and the MediaPro Adaptive Awareness Framework can create a comprehensive model that addresses both organizational and individual user needs in mobile financial services. The structured risk management processes of NIST combined with the adaptive, behaviour-focused training of MediaPro ensure a resilient and aware user base, capable of mitigating cybersecurity threats effectively. The proposed model, termed the Adaptive Governance and Awareness Model (AGAM), integrates the governance and structured approach of NIST with the personalized and adaptive learning of MediaPro.

3.5.1. Identification of Adaptive Governance and Awareness Model (AGAM) Components

Govern: Robust governance policies should be established and aligned with organizational goals. Regulatory compliance and effective risk management must be ensured.

Identify: This component involves educating users about the personal information stored on their phones. Users should be made aware of potential threats, such as phishing or unauthorized access, which can compromise their information. They should be encouraged to keep an inventory of their digital devices and secure the mobile devices used to access financial information.

Protect: Training users on the implementation of strong passwords and the importance of not sharing them with others is crucial. Users should be educated on how to implement biometric and multifactor authentication. Emphasis should be placed on the need for regular updates of financial applications and mobile device operating systems, data encryption on phones, and the importance of using secure connections when using mobile financial services.

Detect: Users should be taught how to recognize unusual activities in their accounts, such as unexpected transactions or login attempts from unexpected devices. Additionally, users should be encouraged to set up notifications and alerts to detect suspicious activities promptly.

Respond: Users should be educated on how to report suspicious activities to their service providers promptly. Guidelines on immediate steps to take if a device is lost or stolen, such as remotely wiping data and notifying their financial service provider or security agencies, should be provided.

Recover: The need for regular backups of financial data and how to restore data after a security incident should be stressed. Users should be encouraged to review and update their security practices regularly, learning from past incidents to enhance their security posture. Users should also be informed about available resources from their financial service provider, such as fraud resolution and customer support services.

Analyse: Evaluating specific threats to mobile financial services, such as phishing, malware, and unauthorized access, is necessary. This includes understanding how users interact with mobile financial services, identifying common mistakes and risky behaviours, determining the current level of awareness, and pinpointing areas where users lack knowledge or exhibit unsafe practices.

Plan: Clear goals for the awareness program should be defined, such as reducing incidents of fraud or increasing user knowledge about secure transactions. Relevant and engaging content that addresses specific security issues identified during the analysis phase should be created. This could include tutorials on enabling two-factor authentication, recognizing fake apps, and avoiding public Wi-Fi for transactions. Effective channels to reach users, such as in-app notifications, SMS alerts, emails, and interactive tutorials within the mobile app, should be chosen.

Train: Users should be actively engaged in learning through personalized training programs tailored to individual user profiles. Training options could include interactive sessions, such as in-app interactive tutorials, webinars, simulations demonstrating potential security threats and how to avoid them, gamification to make learning about security fun and engaging, and scenario-based learning providing real-life scenarios to help users understand the practical application of security measures.

Reinforce: Security awareness should become ingrained in users' daily habits. Techniques to keep users engaged and reinforce learned behaviours should be implemented. Regular reminders and updates about security best practices should be sent through in-app messages, emails, and push notifications. Ongoing challenges, quizzes, and refreshers should be used to reinforce key security concepts. Users should be provided with feedback on their security behaviours, such as alerts when risky actions are detected, and encouraged to make improvements.

3.5.2. Differentiating AGAM from Existing Frameworks

The Adaptive Governance Awareness Model (AGAM) is designed as a distinct, integrative framework that addresses the specific cybersecurity needs of Mobile Financial Services (MFS) users, particularly in the Kenyan context. Unlike the NIST framework, which emphasizes organizational governance and structured risk management, or the MediaPro Adaptive Awareness Framework, which focuses on personalized user training and behavioural reinforcement, AGAM uniquely combines both. It offers a hybrid model that embeds adaptive, user-specific training within a governance structure, ensuring both institutional alignment and context-aware user engagement. Table 3.1 provides a side-by-side comparison of AGAM with the NIST and MediaPro frameworks to illustrate its unique contribution to cybersecurity awareness in the MFS domain.

Table 3.1: Comparative analysis of AGAM, NIST and MediaPro Frameworks

Feature/Component	NIST Framework	MediaPro	AGAM (Proposed)
Governanace Structure	Includes governance in recent updates to align cybersecurity with organizational goals.	Does not explicitly focus on governance.	Embeds governance as a foundational component aligned with local regulatory requirements and MFS strategy.
Risk Identification	Emphasizes structured organizational risk assessment.	Focuses on user-specific behavioural analysis and risk profiling.	Combines organizational risk management with end-user risk profiling tailored to MFS threats.
Personalized Training	Generic, not individualized.	Adaptive, based on user behaviour and awareness gaps.	Delivers customized training based on risk profiles, MFS usage, and behavioural analytics.
Cultural and Regional Context	Globally applicable, but not tailored to specific regions.	Context-neutral, lacks localisation features.	Designed for the Kenyan MFS ecosystem but scalable, addressing cultural, infrastructural, and behavioural factors.
Mobile Financial Services (MFS) Focus	Not specifically designed for MFS.	Not optimized for MFS use cases.	Purpose-built for MFS, addressing mobile-specific threats like SIM swap fraud, app vulnerabilities, etc.
Behavioural Reinforcement	Lacks mechanisms for ongoing behavioural reinforcement.	Includes continuous reinforcement and gamification.	Integrates reinforcement (e.g., in-app prompts, SMS nudges, usage-based reminders) for behaviour change.

Feedback and Improvement	Policy updates driven by incident reporting and audits.	Continuous feedback loop from user performance.	Incorporates real-time feedback from user interactions to refine both governance and training modules.
Training Delivery Channels	Primarily organizational (manuals, workshops, policies).	Digital and interactive (quizzes, simulations, emails).	Multichannel delivery using mobile apps, USSD, SMS, and in-app MFS messaging for inclusivity.
Regulatory Compliance Integration	Strong alignment with global standards.	Minimal integration of compliance or regulation.	Embeds compliance with local regulations (e.g., CBK guidelines, Data Protection Act of Kenya).
Organizational–User Integration	Organization-centric; end-user training is peripheral.	User-centric with minimal integration into organizational governance.	Integrates both levels—strategic governance and individual user engagement—into one adaptive framework.

Source: Compiled by the researcher

3.5.2.1. Graphical representation of the proposed model

Figure 3.3 shows the high-level conceptual view of the proposed model that shows the components of AGAM that can be used to improve the security behaviour of users of mobile financial services. A justification and explanation of the interaction between the components is explained in section 5.4.5.

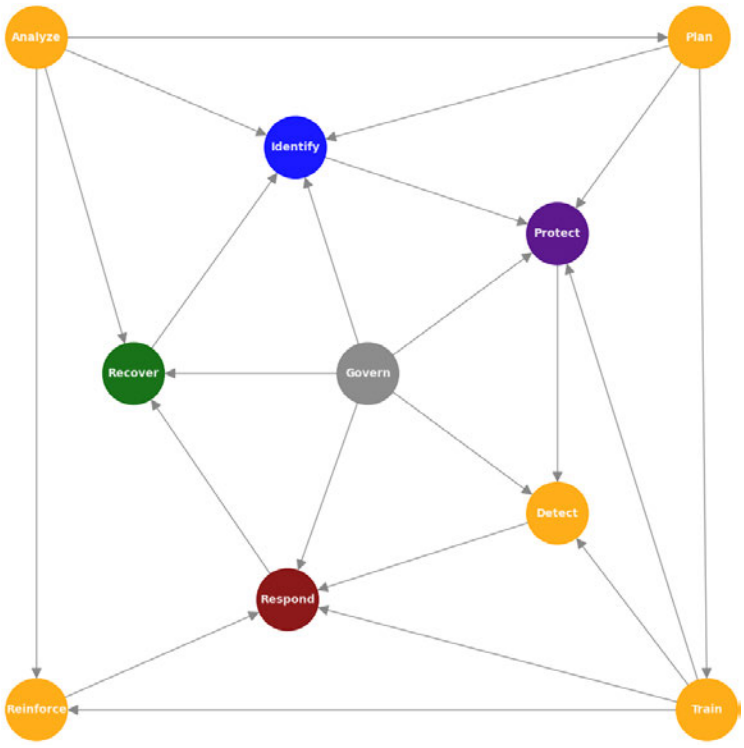


Figure 3.3 Proposed Adaptive Governance Awareness Model (AGAM)

Source: Compiled by the Researcher

3.5.2.2. Relationship between Research Questions, Theoretical Framework and the Questionnaires

Based on the proposed framework for determining the components of Adaptive Governance Awareness Model that can be used to improve the cybersecurity awareness of MFS users, the researcher designed the table 3.2 to show the link between the research questions, the theoretical framework and the questions from the two questionnaires that relate to the constructs identified.

Table 3.2 Link between research objectives, research questions, the proposed theoretical framework and the questionnaires

Research Questions	Theoretical Framework Construct	Questions from the Mobile User's Questionnaire	Questions from the Information Security Professional's Questionnaire
Which concepts and topics on cybersecurity should be included in the Training, Education, and Awareness programmes?	N/A	N/A	N/A
What are the fundamental components of an information security education programme?	N/A	N/A	N/A
How does level of education, age, gender and place of residence influence cybersecurity behaviour of users of MFS	Protect	8,9,10,11,12,13,14,38	4.12, 6.3, 6.4, 6.5, 6.7
	Detect	21,22,43,44,45	6.6, 7.3, 7.6
	Respond	24	
	Recover	15,16,17	
Which constructs borrowed from NIST/MediaPro Adaptive awareness framework can be used to improve	Identify	18, 19, 29,30, 34, 35, 39, 42	6.1, 6.2
	Analyse	14, 15, 16, 19, 23, 31, 32, 33	

awareness among users of MFS	Govern	41, 47, 48	2,3, 4.4, 4.5, 4.7, 4.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6
	Detect	21, 22, 43, 44, 45	6.6, 7.3, 7.6
	Protect	8, 9, 10, 11, 12, 13, 14, 38	4.12, 6.3, 6.4, 6.5, 6.7
	Plan	27, 28.a, 28.b, 28.c, 28.d, 28.e, 28.f, 28.g, 28.h, 28.i, 28.j, 28.k, 28.l, 28.m	3, 4.2, 4.13, 4.14,
	Respond	24	
	Recover	15, 16, 17	
	Train	25,26, 28, 50.a, 50.b, 50.c, 50.d, 50.e, 50.f, 50.g	4.11, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, 5.12, 5.13
	Reinforce	36, 37, 47,49	4.1, 4.3, 4.6, 4.8, 4.10,

Source: Compiled by the Researcher

3.6. CHAPTER SUMMARY

In this chapter, theoretical frameworks related to cybersecurity awareness training are identified. Justifications for the two frameworks used to develop an integrated model for cybersecurity awareness training for users of mobile financial services are then provided. The section concludes by aligning the objectives of this study, the research questions, theoretical constructs (from the frameworks used), and the elements in the research instrument representing the constructs. The following chapter provides a detailed account of how data was gathered.

Chapter 4: Research Methodology

Research is to see what everybody else has seen, and to think what nobody else has thought.

Albert Szent-Gyorgyi

4.1. INTRODUCTION

The Global Information Security Survey report by Ernst and Young (2021) demonstrates that the COVID-19 pandemic compelled many organisations to adopt new customer-facing technologies and cloud-based solutions that facilitated remote work and minimised physical meetings between businesses and clients. The report indicates that the rapid pace of these implementations carried a significant cost, as numerous organisations did not involve the cybersecurity department in decision-making, either due to oversight or urgency to launch or deploy the new service swiftly. Consequently, these new solutions have exposed fresh vulnerabilities that seemingly threaten the businesses. It is becoming increasingly crucial for organisations to consider information security beyond their firewalls, data centres, and employees. The report reveals that mobile devices have bestowed clients with the capability to access resources at any given moment and from any place. As "outsiders become the insiders," individuals external to the conventional corporate framework significantly contribute to achieving an organisation's business objectives, while also potentially posing risks to the safeguarding of the organisation's information resources. As users increasingly utilise mobile devices for work and clients gain access to organisational data via these devices, a growing number of breaches affecting customer data are observed (Ameen et al., 2021). The escalating trend of mobile computing, coupled with the increasing mobile workforce, emphasises the pressing need for an effective Security Education, Training, and Awareness (SETA) programme, as highlighted by Dimov (2017) and Wang et al. (2022), who rated SETA as the most successful approach to preventing cybersecurity incidents in organisations.

Wood (1995) and Dash and Ansari (2022) caution that information security initiatives are destined to fail if the people involved do not support the information security technology solutions adopted, regardless of how effective such solutions may be. The majority of security incidents result from human errors and ignorance rather than malicious intent, indicating that the "human element" remains the most significant security risk in any organisation. In the present digital age, malevolent actors have numerous opportunities to breach the information

systems of individuals, organisations, and governments. Consequently, everyone bears the responsibility to educate themselves about phishing to recognize and defend against phishing attacks (Sonowal, 2022). To mitigate the risks posed by such occurrences, Mobile Financial Services (MFS) providers must devote substantial effort to cybersecurity education and awareness training.

The aim of this study is to develop a model for cybersecurity education, training, and awareness to aid in the enhancement of information security behaviour among users of mobile financial services. In this chapter, the research methods employed to answer the study questions set out for this investigation are presented. This section outlines the nature of this research, research design, research approach, instruments for data collection, the population for this study, the data collection and processing methods, and the NIST Cybersecurity and MediaPro Adaptive Awareness Frameworks. The NIST cybersecurity and MediaPro Adaptive Awareness frameworks have been employed to validate the hypothesis and examine the impact of training in determining user behaviour in the context of employing mobile devices for conducting financial transactions.

4.2. NATURE OF THE RESEARCH STUDY

The central focus of this research study revolves around investigating the significance of Information Security Education, Training, and Awareness (SETA) in augmenting user security behaviours during the process of carrying out mobile financial transactions. The study adopts a comprehensive approach, employing both desk research and a blend of qualitative and quantitative research methods. The qualitative approach relates to the interpretive method of analysing users' and professionals' attitudes, skills, knowledge, and behaviours. Quantitative research has been conducted using questionnaires. Data analysis from the questionnaires was conducted utilising the statistical software SPSS 27.

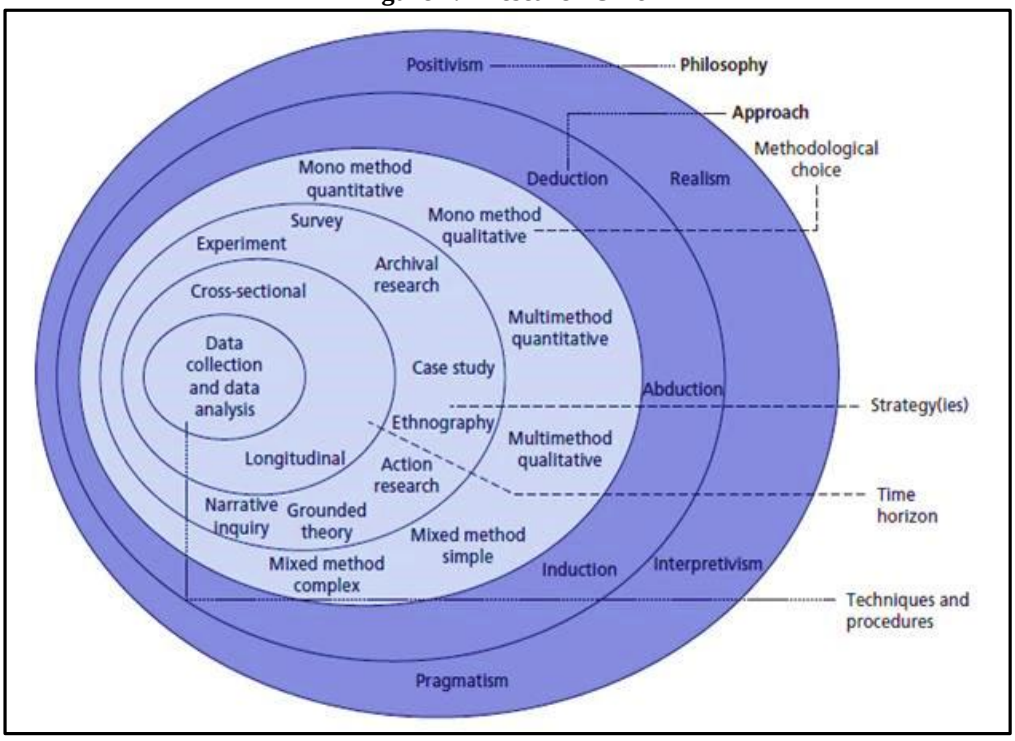
In this study, two distinct questionnaires were employed, each directed at specific groups of respondents. The first group primarily consisted of mobile financial service users, who were the primary focus of the research. The second group included information security professionals and mobile financial solution providers. This approach aimed to enable the validation of certain responses through cross-verification.

The first group involved 1170 respondents, while the second group consisted of 35 information security professionals and solution providers who received the questionnaires.

4.3. RESEARCH DESIGN

Research design refers to the overarching strategy employed to conduct a study, as well as the comprehensive and detailed plan outlining the implementation of that chosen strategy. The research design plays a crucial role in delineating the precise procedures and methods to be employed for data collection, measurement, and analysis throughout the study. An appropriate research design determines the type of data that will be collected, the techniques utilised for data collection, the tools employed for analysis, and the selection of the sample group for the research (Nayak & Singh, 2021). The research onion model proposed by Saunders et al. (2009) served as a guide for this study. The research onion is presented in layers, symbolising the sequential stages that a researcher needs to navigate to craft a robust methodology. At each layer of this model, the researcher conscientiously considered various options and employed sound, logical, and methodological judgment to make the most appropriate decisions. Figure 4.1 depicts the research onion.

Figure 4.1 Research Onion



Source: (Saunders et al. (2009: 108)

This model comprises of six layers. The analogy between the onion and research methodology concerns the orderly process of peeling. For example, if one were to remove every layer of an onion, one would start with the outer layer, peeling off each subsequent layer until reaching

the core. Similarly, in research, the outermost layer of the research onion consists of the research philosophy; from there, progression is made through the intermediate layers, including that of research strategies, until the core is reached, which consists of research procedures.

The research design, guided by the research onion model, involved a structured approach to understanding user awareness in mobile financial services. The selection of two distinct groups, general users of mobile financial services and professionals in information security, allowed for a comprehensive analysis. This dual approach ensured that both the end-user perspective and the insights from service providers were captured, thereby enriching the study's overall validity. In the context of this research, the dual-questionnaire approach was meticulously chosen to align with the research objectives, ensuring that the design facilitated a robust comparison of perspectives between general users and professionals.

4.4. RESEARCH PHILOSOPHY

The initial and fundamental layer of the research onion pertains to the beliefs associated with the nature of the reality under investigation. This stage forms the basis of the research and defines the following terms:

i. Epistemology: The nature and sources of knowledge or facts.
ii. Ontology: The nature of reality.
iii. Axiology: The beliefs, values, and ethics of the specific research.

The choice of a research philosophical stance influences the data collection and analysis processes. However, what do ontology, epistemology, and axiology mean in relation to research philosophy?

4.4.1. Epistemology

In this branch of philosophy, the focus lies on what is (or should be) deemed as acceptable knowledge within a subject area and how it can be acquired. Epistemology seeks to answer questions beginning with "what" and "how." It addresses what we can know about reality and how we can learn about reality and may include questions like "how does one acquire knowledge?" (Nayak & Singh, 2021). Epistemology considers the means to knowledge to include perception, intuition, sensation, reason, and even faith.

Three philosophical stances related to epistemology that help to understand it better are positivism, critical realism, and interpretivism (Mingers, 2006; Saunders et al., 2016). These are as follows:

i. Positivism: This position supports the idea that knowledge in science is acceptable or accurate world knowledge and is usually identified through testing study questions or hypotheses based on existing theories. This philosophical stance is established by replicating a body of research using the same quantitative results from statistical analysis. Schiffman and Kanuk (1997) argue that this is a philosophy of observation and subsequent statistical analysis of the data observed. This philosophy further assumes that the researcher is impartial during the study. This research adopted a positivist approach to research design.

ii. Realism: This philosophy questions the reliability of scientific knowledge. It contends that continuous study and the application of new research methods can generate more reliable results, leading to the revision of theories. Therefore, new research methods will contribute to acceptable knowledge.

iii. Interpretivism: In contrast to realism and positivism, interpretivism emphasises using qualitative methods over quantitative or statistical analysis to acquire results. A researcher employing an interpretivist approach ensures that the data collected is interpreted. Therefore, it is accurate to observe that interpretivism integrates people's interests into a study and recognizes that people are different.

4.4.2. Ontology

Ontology, a branch of metaphysics, is concerned with the study of reality or the aspects of reality. The world's inventory (or ontology) consists of physical objects, properties, values, events, minds, and abstract entities like sets and numbers. This philosophical inquiry addresses the question, "What is?"

Ontology encompasses pragmatism, constructivism, and objectivism, which provide further understanding:

i. Objectivism: This perspective originates from the notion that human values and knowledge are generally impartial, shaped by the nature of reality, and not constructed solely by one's thoughts (i.e., social actor). In the event of rainfall, its reality becomes evident, and all living creatures readily acknowledge its presence. This type of reality

does not depend on one's thoughts, but it does influence them. In research, for example, one might describe how a specific government law would impact people's lives.

ii. Constructivism: This theory focuses on the generation of knowledge and how human decisions and interactions shape ideas. Contrary to objectivism, constructivism maintains that social actors create or depend on reality. For example, a government may enact a new law (reality) because of the actions of a group of people (social actors) who are now affected by the new law.

iii. Pragmatism: This approach focuses on the interplay between theory and practice, highlighting the philosophy that acknowledges the validity and practicality of both constructivism and objectivism as viable approaches in any study. Moreover, these approaches can be effectively employed in problem-solving endeavours.

4.4.3. Axiology

Axiology, a branch of philosophy, is dedicated to the examination of value-related judgments (Saunders et al., 2016). Its main concern lies in evaluating the role of the researcher's values throughout the research process (Li, 2016). Consequently, it primarily focuses on the ethical and valuable aspects as perceived by the researcher. Ethical issues for this research were considered and are described in detail in section 4.8.1.

The researcher maintained his objectivity in this study, by employing scientific methods, including determining causes, and testing hypotheses. The study's hypotheses were formulated based on NIST Cybersecurity framework and MediaPro Adaptive Awareness framework constructs, which offered a lens to investigate the components of the adaptive governance awareness model. The constructs examined in this study include govern, identify, protect, detect, respond, recover, analyse, plan, train and measure and reinforce. The collected data was subjected to tests, allowing conclusions to be drawn.

As presented in Figure 4.2, Patel (2015) offers a comprehensive overview of each paradigm and demonstrates how each research could be situated between the paradigms.

Paradigm	Ontology *What is reality?*	Epistemology *How can I know reality?*	Theoretical Perspective *Which approach do you use to know something?*	Methodology *How do you go about finding out?*	Method *What techniques do you use to find out?*
Positivism	There is a single reality or truth (more realist).	Reality can be measured and hence the focus is on reliable and valid tools to obtain that.	Positivism Post-positivism	Experimental research Survey research	Usually quantitative, could include: Sampling Measurement and scaling Statistical analysis Questionnaire Focus group Interview
Constructivist / Interpretive	There is no single reality or truth. Reality is created by individuals in groups (less realist).	Therefore, reality needs to be interpreted. It is used to discover the underlying meaning of events and activities.	Interpretivism (reality needs to be interpreted) • Phenomenology • Symbolic interactionism • Hermeneutics Critical Inquiry Feminism	Ethnography Grounded Theory Phenomenological research Heuristic inquiry Action Research Discourse Analysis Femenist Standpoint research etc	Usually qualitative, could include: Qualitative interview Observation Participant Non participant Case study Life history Narrative Theme identification etc
Pragmatism	Reality is constantly renegotiated, debated, interpreted in light of its usefulness in new unpredictable situations.	The best method is one that solves problems. Finding out is the means, change is the underlying aim.	Deweyan pragmatism *Research through design*	Mixed methods Design-based research Action research	Combination of any of the above and more, such as data mining expert review, usability testing, physical prototype
Subjectivism	Reality is what we perceive to be real	All knowledge is purely a matter of perspective.	Postmodernism Structuralism Post-structralism	Discourse theory Archaeology Genealogy Deconstruction etc.	Autoethnography Semiotics Literary analysis Pastiche Intertextuality etc.
Critical	Realities are socially constructed entities that are under constant internal influence.	Reality and knowledge is both socially constructed and influenced by power relations from within society	Marxism Queer theory feminism	critical discourse analysis, critical ethnography action research ideology critique	Ideological review Civil actions open-ended interviews, focus groups, open-ended questionnaires, open-ended observations, and journals.

Figure 4.2 Comparison of Research Philosophy

Source: Patel (2015)

The research philosophy, rooted in epistemology, ontology, and axiology, provided the foundational beliefs guiding the study. The choice of a positivist approach reflects the study's emphasis on objective knowledge and replicable results, particularly crucial in assessing user awareness and professional insights into mobile financial services. The ontological and axiological stances further reinforced the research's commitment to understanding user behaviour's objective reality and the findings' ethical implications. By contextualizing these

philosophical stances, the research effectively bridged the gap between theoretical constructs and practical application, ensuring that the methodology was well-suited to the study's aims of developing a user awareness model.

4.4.4. Hypothesis

Hypothesis 1 (H_1): The ability to govern positively influences the ability to identify potential threats.

Hypothesis 2 (H_2): The ability to govern positively influences the ability to protect.

Hypothesis 3 (H_3): The ability to govern positively influences the ability to detect.

Hypothesis 4 (H_4): The ability to govern positively influences the ability to respond.

Hypothesis 5 (H_5): The ability to govern positively influences the ability to recover.

Hypothesis 6 (H_6): The ability to identify potential threats positively influences the ability to protect.

Hypothesis 7 (H_7): The ability to protect positively influences the ability to detect.

Hypothesis 8 (H_8): The ability to detect positively influences the ability to respond.

Hypothesis 9 (H_9): The ability to respond positively influences the ability to recover.

Hypothesis 10 (H_{10}): The ability to recover positively influences the ability to identify potential threats.

Hypothesis 11 (H_{11}): The ability to analyse positively influences the ability to plan.

Hypothesis 12 (H_{12}): The ability to plan positively influences the ability to train.

Hypothesis 13 (H_{13}): The ability to train positively influences the ability to reinforce.

Hypothesis 14 (H_{14}): The ability to train positively influences the ability to protect.

Hypothesis 15 (H_{15}): The ability to plan positively influences the ability to protect.

Hypothesis 16 (H_{16}): The ability to plan positively influences the ability to identify potential threats.

Hypothesis 17 (H_{17}): The ability to analyse positively influences the ability to identify potential threats.

Hypothesis 18 (H_{18}): The ability to analyse positively influences the ability to recover.

Hypothesis 19 (H_{19}): The ability to analyse positively influences the ability to reinforce.

Hypothesis 20 (H_{20}): The ability to reinforce positively influences the ability to respond.

Hypothesis 21 (H_{21}): The ability to train positively influences the ability to detect.

Hypothesis 22 (H_{22}): The ability to train positively influences the ability to respond.

Hypothesis 23 (H_{23}): The ability to reinforce positively influences the ability to recover.

4.5. RESEARCH APPROACH

This layer of the research onion establishes the methods a researcher adopts when conducting a study. The two primary research approaches are deductive and inductive, and the selection depends on research limitations, aims, and researchers' individual opinions.

i. Deductive: This approach typically flows from generic to specific. When a researcher employs a deductive argument, the process begins with theory before addressing study questions or hypotheses, which are then tested through data collection. The data's results either reject or confirm the hypotheses or study questions.
ii. Inductive: This approach or argument type is typically used or beneficial when only limited research is obtainable on a subject. In contrast to the deductive strategy, the researcher employs an inductive approach, progressing from study questions to description and observation, and subsequently, to analysis and theory development.
iii. With respect to inductive research, the researcher aims to deduce patterns and concepts of theory from the observed data. Conversely, in deductive research, the researcher uses newly observed data to test patterns and concepts derived from theory (Nayak & Singh, 2021). The deductive method is commonly associated with quantitative research, whereas the inductive method is often linked to qualitative research.

This study aimed to identify the best set of variables for awareness training for users that would change their information security behaviours while using mobile financial services. To achieve this, this research adopted both quantitative and qualitative methods (Bergman, 2008; Pandey & Pandey, 2021). While the qualitative method encompasses an individual's behaviour in organisations or groups (Hair et al., 2006; Malhotra, 2004), the quantitative research approach focuses on quantifying data and applying statistical methods to the data (Malhotra, 2004). Neuman (2000) provides a summary of the two approaches, as shown in Table 4.1.

Table 4.1 The Characteristics of Qualitative and Quantitative Approaches

Deductive approach (Quantitative Research)	Inductive approach (Qualitative Research)
The objective is to evaluate hypotheses formulated by the researcher	The objective is to discover and encapsulate meanings after the researcher is immersed in data
Systematic development of measures is undertaken prior to data collection, with efforts made to standardise them as much as possible	Measures are usually specific and may be specific to an individual setting or researcher.
The theory predominantly employs a deductive approach and focuses on causal relationships	Theories can be either causal or non-causal and are frequently inductive in nature.
Typically, the analysis is conducted using statistics, tables, or charts, with a discussion on how they relate to the research hypotheses	The analysis is conducted through generalisations, which involves extracting themes from the evidence and organising the data to present a consistent and coherent picture. Hypotheses are subsequently generated from these generalisations.
Concepts are represented as distinct variables within the framework	Concepts may manifest in various forms, such as themes, generalisations, motifs, and taxonomies. However, the primary objective remains the generation of concepts.
Data is presented in the form of numerical values obtained from precise measurements	Data in qualitative research typically consists of words from documents, transcripts, and observations. Despite this, quantification is still utilised in qualitative research methods.
Procedures are generally standardised, and the assumption is made that replication is possible	Research procedures in qualitative studies can be complex and challenging to replicate.

Source: Neuman (2000)

According to Crowther and Lancaster (2012) a deductive research approach is commonly associated with a positivist philosophy. In alignment with this notion and Saunders et al.'s (2009) research onion model, the current study embraced both the deductive approach and the positivist philosophy.

4.5.1. Methodological Choice

This third layer in the model concerns the decision to use qualitative or quantitative methods or to employ a mixture of both. Qualitative research deals with rich data, including opinions, personal accounts, and descriptions, while quantitative research focuses on measurements, quantities, and numbers.

Three methods that researchers can choose from this layer include:

i. Mono-method: The researcher collects either quantitative or qualitative data depending on the selections made in the research onion's previous steps.
ii. Mixed-method: The researcher uses both quantitative and qualitative data collected during the study. This method is popular since the two approaches attempt to complement each other, thereby overcoming the weaknesses of each specific method.
iii. Multi-method: Data is collected using both quantitative and qualitative techniques. However, the data collected is analysed from one perspective only.

This present research project employed a mixed-methods approach. Combining both provides strengths to balance the respective limitations of qualitative and quantitative techniques (Creswell & Plano-Clark, 2007; Johnson & Christensen, 2008; Nayak & Singh, 2021). In contrast to a singular approach, this method provides a more comprehensive understanding of research problems (Creswell & Plano-Clark, 2007; Johnson & Onwuegbuzie, 2004).

4.6. RESEARCH STRATEGY

This layer of the research onion pertains to plans for data collection, which may include experiments, grounded theory, action research, case studies, archival research, surveys, and ethnography. Researchers may employ multiple methods. Melnikovas (2018) describes these research strategies as follows:

i. Experiment: This strategy is scientific and features a rigid structure. Experimental designs are utilised to examine the cause-and-effect relationships between variables by

manipulating an independent variable and observing its impact on a group or individuals. Data collected through this method can be subjected to statistical analysis.

ii. Case Study: Case studies provide exceptional samples of cases or real people in actual conditions. The number of case studies in research is usually limited to facilitate drawing explicit conclusions from the data.

iii. Survey: A survey design originates from a deductive approach, allowing for the collection of a substantial amount of data that is well-suited for analysis employing statistical methods. The data collected assists in answering the hypothesis or research question economically.

iv. Grounded Theory: This approach collects data for building theory instead of refining or testing one. Using the grounded theory strategy, the researcher typically begins with qualitative data collection or a research question. Finally, the researcher reviews the data collected through observation, and the recurring concepts are coded or organised into groups that sequentially form the basis for a new theory.

v. Action Research: Action Research aims to address an issue in a given situation. It begins by setting a concise goal, followed by a thorough problem diagnosis. Finally, a list of possible solutions is developed and presented as suggestions for resolving the problem.

vi. Archival Research: This strategy derives data from archived documents and existing data. The challenge with this research strategy is that the researcher might hit a dead end because the amount of available information and its accuracy could present difficulties. Therefore, relying solely on secondary data sources is not advisable.

vii. Ethnography: This approach involves studying people in their everyday environment to establish a theory or hypothesis around culture and behaviour. The researcher becomes part of the community under investigation to uncover facts about long-term changes in actions and opinions. This study design is time-consuming and somewhat daunting.

This research employed the survey approach for data collection. Data were collected using two different types of questionnaires. One was distributed to MFS users to determine their security behaviours, knowledge, and skills regarding mobile financial security and risks. The second questionnaire was aimed at information security professionals working in institutions offering mobile financial services. Its purpose was to assess their cybersecurity awareness and

training efforts. Additionally, the questionnaire aimed to validate and corroborate the information and data provided by mobile financial services users. The two questionnaires supplied quantitative data to obtain reliable, generalisable, and statistically valid results.

4.7. TIME HORIZON

This is the fifth layer and addresses the study's timeframe. Researchers have two options from which to choose: longitudinal or cross-sectional.

i. Longitudinal: The researcher is interested in studying behaviours and events over a long time using concentrated samples.
ii. Cross-sectional: In this option, the researcher examines an issue at a specific time, and the duration of data collection and the study period are limited to a short span.

The present study utilised a cross-sectional approach for the research timeframe.

4.8. RESEARCH TECHNICS AND PROCEDURES

The outermost layer of the research onion pertains to methods for collecting and analysing data. This section addresses decisions on sample groups, the contents of questionnaires, interview questions, and ethical considerations.

The researcher employed the Kolmogorov-Smirnov test to evaluate the normal data distribution within each question based on predictions of a Gaussian distribution. To determine the internal consistency of questions with the same scale, Cronbach's Alpha test was utilised. This test serves to assess reliability and ascertain data quality. Specifically, the Cronbach's alpha test was applied to the MFS subscriber's questionnaire, computed for all questions of the same scale in each section. Assessing consistency and reliability aided in determining the overall data quality. Satisfactory results were indicated by Cronbach's Alpha values of 0.7 or higher for all questions. The outcomes of the data collection instruments for this study are presented in Table 4.2.

Table 4.2 Results of Cronbach's Alpha Reliability Analysis: Questionnaire for MFS Subscribers

Questions	Similarity of Scale	Cronbach Alpha
8B,10B-16,18,19,22,25,2932,34,36-42,44,45,47-49	Yes/No	0.802
4B, 7B,17,20,35,43	Very small extent – Very large extent	0.711

Source: Compiled by the Researcher

4.8.1. Ethical Considerations

The University of KwaZulu-Natal (UKZN) emphasises the importance of ethical practice standards for all researchers conducting studies. Researchers are expected to adhere to these ethical guidelines to ensure the protection of human subjects, maintain integrity in research, and uphold the highest ethical principles throughout their studies. Before data collection, the researcher sought clearance from the gatekeepers, specifically, the Communication Authority of Kenya (CAK) and Safaricom Limited.[3] After receiving clearance from these institutions, the researcher applied to the Research Office of UKZN and was granted permission to proceed with the study.[4] The researcher obtained clearance number HSS/1508/015D. Gauthier (2005) suggests the following principles concerning ethics, which the researcher followed during the study:

i. Integrity.
ii. Scientific, professional, and social responsibility.
iii. Upholding the rights and dignity of individuals.
iv. Competence.
v. Demonstrating care for the well-being of others.

The data collection instruments included an accompanying cover letter informing respondents that their answers would remain confidential and undisclosed. Consequently, respondents' personal data were not used. The researcher also employed research assistants who assisted

[3] See: Annexure D and Annexure E.
[4] See: Annexure K.

respondents and explained any questions they could not understand. The participants were explicitly notified that their participation was voluntary, without any financial incentives provided. They were equally free to withdraw from participation should they wish.[5]

4.8.2. Target Population and Sample Selection

The target population comprises the entire collection of relevant elements or individuals for a study, and the researcher aims to generalise conclusions based on this group (Hair et al., 2006; Pandey & Pandey, 2021). The target population in this research consisted of mobile financial service users and information security professionals who work in organisations that provide these services to the users. In this study, they acted as the principal agents for data collection. However, the population of individuals who use MFS is distributed across the country.

Sekaran and Bougie (2010) recommend adopting cluster sampling when the target population is spread out over a large area. Cluster sampling allowed the researcher to divide the population into distinct groups called clusters. In cluster sampling, the clusters must contain a heterogeneous mix of individuals (Leedy & Ormrod, 2010). This method is a good representative of the population, highly economical, and the observation can be used for inferential purposes (Pandey & Pandey, 2021).

In this research, the population was divided into clusters of cities. A sample of five cities was chosen to represent the cities. These cities represent broader demographics such as age, gender, level of education, income levels, and ethnic diversity, ensuring that the data gathered can be applied to the wider population. Furthermore, these cities are commonly utilized by the government and government agencies to conduct research, providing a basis for comparison and longitudinal analysis.

Table 4.3 presents the population of the country and the population of the major cities selected for the survey. Table 4.3 also displays the number of questionnaires sent to each city.

[5] See: Annexure G and Annexure H.

Table 4.3 Population in the Sampled Cities (2019 Population Census)

Area	Current Population (2019 Census)	Questionnaires Distributed	% of Population and Questionnaires
Kenya	47,564,300		
Nairobi city	4,397,073	510	43.10
Nakuru	2,162,202	210	18.10
Mombasa	1,208,333	150	12.93
Kisumu	1,155,574	150	12.93
Eldoret	1,163,186	150	12.93

Source: KNBS (2019)

After the clusters were identified, random sampling was utilised in distributing the questionnaires among participants. In random sampling, each item in the population has an equal and independent probability of being selected for inclusion in the sample (Cooper & Schindler, 2008; Pandey & Pandey, 2021). This technique, therefore, ensured that every participant had an equal opportunity of being selected from the population (clusters). A total of 1170 questionnaires were distributed, of which 1, 159 were returned, representing a 99.06% response rate. The 99.06% response rate was achieved as research assistants followed up with respondents to ensure the return of all questionnaires.

Sample size Justification

In this study, a total of 1,170 questionnaires were distributed to a target population of 10,086,368 of mobile financial users from the selected five cities. The selection of this sample size was guided by statistical principles to ensure representativeness and the ability to generalise findings to the entire population.

To determine the appropriate sample size, the following factors by Cochran (1977) were considered:

- **Confidence Level**: A standard confidence level of 95% was selected, which is commonly used in social sciences research. This implies that there is a 95% probability that the sample accurately reflects the population.
- **Margin of Error**: A margin of error of 3% was chosen to balance precision and feasibility. The margin of error represents the range within which the true population parameter is expected to fall.

- **Population Proportion (P)**: A conservative estimate of 50% was used for the population proportion. This value maximizes the sample size, providing the most robust estimate when the proportion of the population that exhibits the characteristic of interest is unknown.
- **Sample Size Formula**: The sample size was calculated using the following formula for a finite population:

$n = (z)^2 \, p \, (1 - p) / E^2$

Where:

- n is the sample size,
- Z is the Z-value corresponding to the desired confidence level (1.96 for 95% confidence),
- P is the estimated population proportion (0.50 in this case),
- E is the margin of error (0.03 for 3%).

Substituting the values:

$n= (1.96)^2.0.5.(1-0.5)/(0.03)^2=1,067$

To account for non-responses or unusable questionnaires, the sample size was increased by approximately 10%, resulting in a final sample size of 1,170.

This sample size ensures adequate statistical power to detect significant relationships and supports the generalizability of the study's findings to the broader population of mobile financial services users.

4.8.3. Pilot Study

A pilot study denotes a preliminary trial carried out by a researcher in readiness for the primary research (van Teijlingen & Hundley, 2001). The central goal of this preliminary investigation is to pick out potential deficiencies in the design of data collection tools. Involving respondents from the target population, a pilot study simulates the data collection processes and adheres to the established rules for data gathering (Cooper & Schindler, 2008).

In this study, a pilot investigation was conducted to assess the questionnaire's effectiveness, aimed at identifying and rectifying any potential issues such as misunderstood questions, unexpected responses, and difficulties encountered while filling the questionnaire. It aimed to determine if users clearly understood the questions and instructions. The pilot study size may

involve subjects ranging from 25 to 100 subjects (Cooper & Schindler, 2008). In this feasibility study, we administered a total of 200 questionnaires to users of mobile financial services residing in five major cities, and an additional 26 questionnaires were distributed to information security professionals. Out of the distributed questionnaires, 146 completed responses were received from mobile financial service users, and 18 completed responses were received from the information security professionals. After removing incomplete responses, 109 from users and 11 responses from information security professionals were deemed usable. The pilot study revealed that some amendments were necessary for the data collection instruments.[6]

4.9. DATA COLLEECTION METHODS

The main method of data collection utilised in this research involved the administration of questionnaires. The fieldwork lasted three months, from September 2020 to December 2020. The researcher enlisted the assistance of research assistants from the respective cities to help distribute and administer the questionnaires. A total of 1,170 questionnaires were distributed to mobile financial users, of which 1,159 were returned, yielding a 99.06% return rate. Additionally, 35 questionnaires were sent to information security professionals, with 23 being returned, reflecting a 65.71% return rate. The user questionnaire was divided into two parts. Part one of the questionnaire collected demographic data from each respondent, while part two gathered data about knowledge regarding information security concepts.

Questionnaires can have both advantages and disadvantages. Gay (1992) and Pandey and Pandey (2021) identify some of these in Table 4.4.

[6] These changes were incorporated into the final questionnaire. See: Annexure G and Annexure H.

Table 4.4 Advantages and Disadvantages of Questionnaires

Advantages	Disadvantages
It is easy to administer, and respondents can quickly fill in	Analysis of data from the questionnaire consumes time
Follow-up is easy	It is not easy to get a list of good questions together
It is easy to quantify data	Some respondents do not give honest answers
Making responses tabulation is quite effortless	The effectiveness of questionnaires is dependent on individuals reading ability and comprehension
Enables the direct comparison of individuals and groups	Due to fear of lack of anonymity, the response rate is usually low.
It is suitable for large samples	Questions that explore in depth are difficult to get
It gives direct attitudinal and information responses	Respondents usually give what they feel is the "correct response."

Source: Adapted from Gay (1992) and Pandey and Pandey (2021)

In this study, despite the acknowledged disadvantages of using questionnaires, the researcher took great care in their construction to ensure simplicity and clarity. The questionnaire design deliberately avoided excessively long questions and included only straightforward inquiries that could be comfortably answered, while following a natural order and logical progression. All possible answers were also covered in the questionnaires.

4.9.1. Research Questions

This part of the research paper connects the techniques for data collection, research questions, and expected data outcomes. Furthermore, this research also gives a comprehensive explanation of the statistical methods utilised to address the research questions.

4.9.2. Testing of Hypothesis

Hypotheses were formulated and subjected to testing, aiming to enhance the comprehension of the research. Normality tests were performed to determine the suitable statistical analysis for the data. Comprehensive results of these tests can be found in chapter five of this research study. The following hypotheses were examined using the Kolmogorov-Smirnov test:

H_0: the tested variables are derived from a normal distribution.

H_1: the tested variables are not derived from a normal distribution.

4.9.2.1. Logistic Regression

To address Question #4, Logistic Regression was utilised to investigate the attributes that influence secure behaviour of users when using MFS. This study used logistic regression for several categorical explanatory variables and the binary variable. Question #49 in the MFS subscribers' questionnaire served as the binary response variable, i.e., Do you think there is a need for mobile Security Education Training and Awareness in Kenya? The explanatory variables included age, level of education, prior financial loss experience, and gender.

Table 4.5 The Link between Data Collection Techniques, the Research Questions, and the Expected Data Outcomes

Research Question	Research Method	Expected Data
Which concepts and topics on Information Security could constitute part of the Infosec Training, Education and Awareness?	• Structured Questionnaire used in this study. • Analysis of documents from governments, books, journals, conference proceedings, websites, databases.	• Insight from users and professionals. • Evidence from documents.
What are the fundamentals of an information security programme?	• Structured Questionnaire used in this study. • Analysis of documents from governments, books, journals, conference proceedings, websites, databases.	• Insight from users and professionals • Evidence from documents
How does level of education, age and place of residence influence cybersecurity behaviour of users of mobile financial services?	• Structured Questionnaire used in this study. • Analysis of documents from governments, books, journals, conference proceedings, websites, databases.	• Insight from users and professionals • Evidence from documents • Analysis and validation of the data through statistical procedures

Research Question	Research Method	Expected Data
Which constructs borrowed from NIST Cybersecurity and MediaPro Adaptive Awareness frameworks can be used to improve cybersecurity awareness among users of mobile financial services?	• Structured Questionnaire used in this study. • Analysis of documents from governments, books, journals, conference proceedings, websites, databases	• Insight from users and professionals • Evidence from documents • Validation of the proposed model

Source: Compiled by the Researcher

4.9.3. Data Collection Instrument

This study employed the use of two questionnaires.

i. Questionnaire for users of Mobile Financial Services. This questionnaire had two parts. The initial segment involved gathering demographic data from the respondents, while the subsequent part aimed to assess the respondents' understanding of information security concepts. The questions were closed. The researcher chose closed questions since they are easier to code and analyse statistically and more straightforward and quicker for respondents to answer. It is also easy to compare responses from different respondents.

Some questions had follow-up questions. An extracted example is provided in Figure 4.3.[7]

25. Have you ever attended an awareness session on mobile security?
    a) Yes [ ]
    b) No [ ]
26. If **YES** in 25 above, to what extent did you like the awareness session (i.e. was the awarenes helpful to you)?
    a) Yes [ ]
    b) No [ ]
27. If **NO** in 26, what didn't you like in the awareness session? Tick ALL that apply.
    a) Content was not appropriate [ ]
    b) Mode of training was not appropriate [ ]
    c) It was not interesting [ ]
    d) Any other (Please specify) [ ]

Figure 4.3 Extract from Questionnaire for Users of Mobile Financial Services

Source: Compiled by the Researcher

Questionnaire for Providers of Mobile Financial Services: This questionnaire targeted information security professionals who work in organisations that provide mobile financial services. The questionnaire was meant to investigate their efforts in improving the information security behaviours of users and the challenges they have experienced in the process.

The data gathered from these two questionnaires would help identify the gaps and inform the decision to develop an adaptive model for SETA.

[7] Please note: The question numbering has been adjusted to reflect tabulated forms used elsewhere within the body of this research study.

4.10. DATA ANALYSIS

The data collected was analysed using the Statistical Package for the Social Sciences (SPSS). The process of analysis included the following:

i. Data Cleaning: This involved checking for missing values and the existence of all data.
ii. Data Coding: This involved assigning number values to each variable.
iii. Descriptive Analysis: This was done to understand each of the data.
iv. Graphs: Graphs were generated to provide a graphical view of the data
v. Cross Tabulation: This was used to summarise the relationship between variables. It was mainly used to examine the relationships within the data that were not apparent during the analysis of survey responses.
vi. Logistic Regression: This was employed in answering the study question: Does SETA impact the security behaviour of MFS users and providers? This study also used logistic regression to test the connection between the explanatory and binary variables.
vii. Correlation Analysis: The analysis was conducted on specific variables to ascertain the direction and strength of the relationship between them. The analysis showed either positive or negative correlations in those situations.
viii. Structured Equation Modelling: The analysis was performed to establish the structural connection between the measured variables and the latent constructs in the theoretical research model.
ix. The Kolmogorov Smirnov: This was conducted to establish if samples came from a population with normal distribution.
x. Mann Whitney U and the Kruskal Wallis Test: This was employed in testing if there are notable differences between the demographic variables.

4.11. CHAPTER SUMMARY

This chapter elucidates the research methodology used in the current study. Furthermore, through the utilisation of the research onion framework, it emphasises the research design as proposed by Saunders et al. (2009). In this study, a combination of qualitative and quantitative methods of data collection were employed to identify the constructs necessary for developing an Adaptive Governance Awareness Model (AGAM). To gather quantitative data, a survey instrument was designed, tested, and administered. Subsequently, the collected data underwent statistical analysis. The quantitative data was also used to validate the hypotheses. The next

chapter presents concepts and topics on information security that could be included in cybersecurity education and awareness training programme.

Chapter 5: Research Findings and Analysis of Results

Supposing is good, but finding out is better.

Mark Twain

5.1. INTRODUCTION

This chapter will offer an in-depth analysis of the gathered data with the primary aim of achieving the research objectives and addressing the research questions comprehensively. The data will undergo a descriptive analysis, which will be accompanied by a discussion of the results in light of the existing literature. Additionally, quantitative representations in the form of graphs, charts, and tables will be utilised to provide clear visualisations of the findings.

5.2. PROFILE OF THE MOBILE FINANCIAL USER IN THIS STUDY

5.2.1. Hypothesis Testing

Hypotheses were developed and subsequently tested as part of the study to gain deeper insights into the research topic. To determine the appropriate statistical analysis, normality tests were conducted on the data. Detailed explanations and descriptions of these results are elaborated upon in the subsequent sections of the research report.

5.2.2. Kolmogorov Smirnov Test

The research study involved testing the following hypotheses:

H_0: The tested variables originate from a normal distribution.

H_1: The tested variables do not originate from a normal distribution.

Table 5.1 Kolmogorov Smirnov Test for Significance

	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
1. Gender.	12.322	.000
2. Age.	8.331	.000
3. What is your highest level of education?	6.123	.000
4. How can you best describe your main place of residence?	8.197	.000
5. For how long you have owned a mobile phone?	8.290	.000
6. Who is your service provider? You can select more than one if applicable.	8.001	.000
7. Which of the following services do you access on your phone? (Tick all that apply)	10.035	.000
8. To what extent do you trust the mobile platform when undertaking a financial transaction?	9.982	.000
9. How often do you seek assistance from people with your phone to carry out MPESA/Mobile money transactions?	13.423	.000
10. On a scale of 1-5, how would you rate your confidence when using your phone to perform MPESA/Mobile money transactions without requiring help from someone else?	9.481	.000
11. To what extent do you feel money kept in your mobile wallet is safe from theft/loss?	7.516	.000
12. Are you aware that your phone has settings that allows you to auto-lock your phone when it is not in use for some time?	17.310	.000

	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
13. Are you aware that you can set a password that is not easy to guess for your phone or mobile money (for example not using date of birth or repeating digits in your password)?	17.442	.000
14. Do you know how to physically secure your phone i.e., Put an auto lock password and require password to unlock without help?	17.958	.000
15. Does your mobile phone have any password/security code for locking?	16.221	.000
16. Are you aware you should not use the same security code/password for mobile money to access your social other networks e.g., E-mail, Facebook, Twitter accounts, google etc.?	17.286	.000
17. Are you aware you can change your MPESA PIN/password as often as you want?	17.569	.000
18. Have you shared your mobile money PIN/Password with others to perform a transaction?	13.562	.000
19. Have you shared your phone with someone to help you with a transaction?	13.818	.000
20. Have you shared your government registration ID card/Passport to someone to withdraw MPESA for you?	14.417	.000
21. To what extent are you concerned that someone could use your ID and do a SIM swap and use it to commit fraud?	7.963	.000
22. Are you aware that you are not supposed to keep your MPESA PIN/Mobile Bank password as a draft message on your phone?	17.430	.000
23. Have you set your phone to show password/PIN when entering it (so you can easily know what you typed)?	12.746	.000

	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
24. To what extent are you concerned that when you share/or when someone gets to know your password/PIN, they can use it to later commit fraud/remove money from your account/mobile wallet without you knowing?	8.083	.000
25. To what extent do you think you can recognize if your phone has been hacked?	8.131	.000
26. Have you ever lost money through a Mobile money transaction?	11.898	.000
27. If so, what caused you to lose money (Tick all that apply)?	7.618	.000
28. How did you report if you have lost money via MPESA/mobile banking?	9.918	.000
29. Have you ever attended an awareness session on mobile money security?	14.950	.000
30. If YES in #29, did you like the awareness session (i.e., was the awareness helpful to you)?	10.607	.000
31. If NO in #30, what did you not like in the awareness session? Tick all that apply.	13.424	.000
32. Which of the following is your most preferred awareness delivery method? Tick your best three.		
a. Posters.	15.235	.000
b. Periodic SMS blasts.	15.366	.000
c. Person-to-Person interaction.	16.397	.000
d. Television adverts.	13.312	.000
e. Radio announcements in my local dialects.	14.349	.000
f. Road shows in our local area.	17.081	.000

	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
g. Newsletter.	17.861	.000
h. Newspaper adverts.	17.902	.000
i. Classroom workshops.	18.301	.000
j. E-mail.	17.528	.000
k. Web-based training.	18.286	.000
l. Online discussion.	17.662	.000
m. Video-based methods.	18.213	.000
33. Do you keep personally identifiable information (e.g., your name, bank account number etc.) on your phone?	13.611	.000
34. Do you use your phone to access the internet i.e., Facebook, Twitter, Yahoo mail, Google etc.?	17.415	.000
35. Do you enable location services on your phone?	13.474	.000
36. Have you ever downloaded applications and documents from the internet unintentionally or unknowingly?	12.870	.000
37. To what extent do you trust the safety of websites you normally access through your phone?	7.094	.000
38. Does your phone have an antivirus programme?	8.759	.000

	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
39. To what extent are you concerned that some files you download might collect some data from your phone without your knowledge?	6.135	.000
40. Are you aware of any security risks associated with using mobile devices?	15.936	.000
41. Are you aware you can disable location settings on your phone?	16.033	.000
42. Do you know how to change settings/location services on your phone?	16.795	.000
43. Do you think information/ data in your phone is important?	17.778	.000
44. Have you ever heard of mobile security?	15.550	.000
45. Do you know your roles and responsibilities in ensuring secure mobile financial service?	14.717	.000
46. Do you have an idea of any 'social engineering' tricks for mobile devices or what it means?	13.490	.000
47. To what extent do you think you can identify a mobile money hoax (scam) i.e., someone's asking you to pay some money to get a prize or posing as a friend and that they are stuck and needs some money?	8.633	.000
48. Have you encountered a phishing attack (i.e., someone asking for your MPESA PIN, National ID etc.?	14.584	.000
49. Have you had/experienced a vishing attack i.e., someone asking you to call them to claim some money that you have won or someone sending you a message with instructions on how to claim some money you have won?	14.740	.000
50. If YES in #49 above, how did you respond?	13.582	.000
51. Do you think mobile money security awareness is a challenge that needs to be addressed?	18.246	.000

	Kolmogorov-Smirnov Z	Asymp. Sig. (2-tailed)
52. Are you aware of any laws governing mobile security in Kenya?	11.946	.000
53. Do you think there is a need to have a mobile security education training and awareness in Kenya?	17.479	.000
54. If YES in #53, on a scale of 0-5 (0-1 Do not know, 1- Least priority, 5- High priority), how would you want the following information security concepts to be considered for training and awareness?		
a. Physical protection of mobile devices.	6.795	.000
b. Vulnerabilities/Password confidentiality.	8.583	.000
c. Emerging threat and detection (Phishing and vishing schemes)?	8.628	.000
d. MFS fraud incident early detection.	7.274	.000
e. Damage/Loss caused by use of mobile money use, failure, malfunction, interruption, or unavailability of the mobile financial system.	7.900	.000
f. Strong security password setup.	8.356	.000
g. Mobile money risks (theft of phone, money sent to wrong number, PIN leakage to another person, fake money from agent, fake transaction detections.	9.906	.000

Source: Compiled by the Researcher

The Kolmogorov-Smirnov (K-S) test was conducted to assess the normality of various variables related to mobile phone usage and security. The test statistics (K-S Z) and corresponding asymptotic significance values (p-values) were presented for each variable. A p-value less than 0.05 indicated a significant deviation from a normal distribution. In this dataset, all variables exhibited a p-value of 0.000, signifying that the null hypothesis of the data following a normal distribution was rejected for all variables. This implies that none of the variables conformed to a normal distribution.

The results of the Kolmogorov-Smirnov test indicated that all examined variables significantly deviated from a normal distribution. This necessitated the use of non-parametric methods for further statistical analysis in the study. The diverse range of K-S Z values highlighted the varying degrees of non-normality across different aspects of mobile phone usage, security awareness, and experiences with mobile money transactions. This comprehensive analysis can inform the development of targeted interventions and policies to enhance mobile security practices among users.

Due to the significant deviation from normality, non-parametric statistical methods were employed. These included the chi-square test, and the Mann-Whitney U test, which were applied where the situation deemed necessary. Some variables could not be assessed using the Kolmogorov-Smirnov test due to a variance of zero, resulting from one response dominating the data on those variables. Consequently, the test statistic could not be calculated for these cases. For hypotheses testing, the chi-square goodness of fit test was used.

The findings from the Kolmogorov-Smirnov test underscore the importance of using appropriate statistical methods that do not assume normality in the analysis of mobile phone usage and security data. The rejection of the null hypothesis for all variables suggests significant non-normality, necessitating the application of non-parametric tests. This approach ensures the robustness and validity of the statistical inferences drawn from the data, ultimately contributing to more effective strategies and policies in mobile security practices.

5.2.3. Reliability Test

The reliability of various constructs derived from the mobile user's questionnaire was assessed using Cronbach's Alpha. The results are crucial for determining the internal consistency of the items within each construct. The findings are presented in Table 5.2

Table 5.2 Results of Cronbach's Alpha Test

Research Questions	Theoretical Framework Construct	Questions from the Mobile User's Questionnaire	Cronbach's Test
How does level of education, age, gender and place of residence influence cybersecurity behaviour of users of MFS	Protect, Detect, Respond, and Recover	8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 21, 22, 24, 38, 43, 44, 45	0.721
Which constructs borrowed from NIST/MediaPro Adaptive awareness framework can be used to improve awareness among users of MFS	Identify	18, 19, 29, 30, 34, 35, 39, 42	0.667
	Govern	41, 47, 48	
	Analyse	14, 15, 16, 19, 23, 31, 32, 33	0.771
	Plan	27, 28.a, 28.b, 28.c, 28.d, 28.e, 28.f, 28.g, 28.h, 28.i, 28.j, 28.k, 28.l, 28.m	0.734
	Train, Measure and Reinforce	25, 26, 36, 37, 47, 49, 50.a, 50.b, 50.c, 50.d, 50.e, 50.f, 50.g	0.797

Source: Compiled by the Researcher

The reliability of the data was assessed using the Cronbach's Alpha test, a standard measure to determine internal consistency. The widely accepted threshold for Cronbach's Alpha is 0.7 (Gliem & Gliem, 2003), with values above this threshold indicating good reliability. This analysis involved calculating Cronbach's Alpha for all questionnaire items to determine whether the variables in question adequately explained the constructs being measured.

The results of the Cronbach's Alpha test for various constructs indicated varying degrees of internal consistency. Constructs such as 'Protect, Detect, Respond, and Recover' and 'Train, Measure, and Reinforce' demonstrated good reliability, with alpha values exceeding 0.7. This suggests a high level of internal consistency among the items within these constructs. Conversely, the 'Identify' construct displayed moderate reliability, with alpha values below the 0.7 threshold. This indicates potential areas for improvement within this construct, suggesting that the items may not be as cohesively related as those in other constructs.

Overall, the findings from the Cronbach's Alpha test provide a robust foundation for further analysis and validation of the constructs used in this study. The results offer valuable insights into the internal consistency and reliability of the questionnaire items related to cybersecurity

behaviour and awareness. By identifying constructs with high reliability, the study ensures that the measures are dependable and can be confidently used for further research.

5.2.4. Testing for Significant differences

Based on the results of the Kolmogorov-Smirnov test (shown in Table 5.1), non-parametric statistics were employed by the researcher. The Mann-Whitney U were utilized to assess significant differences between the demographic variables.

5.3. MANN-WHITNEY U TEST

H_0: There is no difference between males and females in their cybersecurity behaviour with respect to mobile financial services (MFS)

H_1: There is a difference between males and females in their cybersecurity behaviour with respect to mobile financial services (MFS)

Table 5.3 Significance Based on Mann-Whitney U Test and Cybersecurity Behaviour

Questionnaire Questions	Mann-Whitney U Test	Z	Asymp. Sig. (2-tailed)
Age	150227.500	-3.115	0.002
What is your highest level of education?	166322.500	-0.091	0.928
How can you best describe your main place of residence?	159942.500	-1.294	0.196
For how long have you owned a mobile phone?	149359.000	-3.228	0.001
Who is your service provider? You can select more than one if applicable.	162690.000	-0.768	0.442
Which of the following services do you access on your phone? (Tick all that apply)	153827.000	-2.371	0.018
To what extent do you trust the mobile platform when undertaking a financial transaction?	159719.000	-1.317	0.188
How often do you seek assistance from people with your phone to carry out MPESA/Mobile money transaction?	163527.500	-0.698	0.485

Questionnaire Questions	Mann-Whitney U Test	Z	Asymp. Sig. (2-tailed)
On a scale of 1 to 5, how would you rate your confidence when using your phone to perform MPESA/Mobile money transaction without requiring help from someone else?	161037.000	-1.092	0.275
To what extent do you feel money kept in your mobile wallet is safe from theft/loss?	153806.000	-2.375	0.018
Are you aware that your phone has settings that allows you to auto-lock your phone when it is not in use some time?	160186.500	-1.840	0.066
Are you aware that you can set a password that is not easy to guess for your phone or mobile money (e.g., not using date of birth or repeating digits in your password)?	164895.000	-0.609	0.543
Do you know how to physically secure your phone i.e. Put auto lock password and require password to unlock without help?	160109.500	-2.187	0.029
Does your mobile phone have any password/security code for locking?	151532.000	-3.819	0.000
Are you aware you should not the same security code/password for mobile money to access your social other networks e.g. E-mail, Facebook, Twitter accounts, google etc.?	159560.500	-2.004	0.045
Are you aware you can change your MPESA PIN/password as often as you want?	157800.500	-2.633	0.008
Have you shared your mobile money PIN/Password with others to perform a transaction?	160110.000	-1.401	0.161
Have you shared your phone with someone to help you with a transaction?	160215.500	-1.389	0.165
Have you shared your government registration ID card/Passport to someone to withdraw MPESA for you?	155930.000	-2.339	0.019
To what extent are you concerned that someone can use your ID and do a SIM swap and use it to commit fraud?	159621.500	-1.313	0.189
Are you aware that you are not supposed to keep your MPESA PIN/Mobile Bank password as a draft message on your phone?	156362.500	-2.965	0.003
Have you set your phone to show password/PIN when entering it (so you can easily know what you typed)?	164952.000	-0.385	0.700

Questionnaire Questions	Mann-Whitney U Test	Z	Asymp. Sig. (2-tailed)
To what extent are you concerned that when you share/or when someone gets to know your password/PIN, they can use it to later commit fraud/remove money from your account/mobile wallet without you knowing?	161722.500	-0.939	0.348
To what extent do you think you can recognize if your phone has been hacked?	164982.500	-0.336	0.737
Have you ever lost money through a Mobile money transaction?	160450.000	-1.298	0.194
If so, what caused you to lose money (Tick all that apply)?	153545.000	-2.418	0.016
How did you report if you have lost money via MPESA/mobile banking?	163323.000	-0.661	0.508
Have you ever attended an awareness session on mobile money security?	163562.500	-0.719	0.472
If YES in 25 above, did you like the awareness session (i.e., was the awareness helpful to you)?	158821.000	-1.479	0.139
If NO in 26 above, what didn't you like in the awareness session? Tick all that apply.	162809.500	-0.770	0.441
Which of the following is your most preferred awareness delivery method? Tick your best three.	165818.500	-0.086	0.931
POSTERS			
PERIODIC SMS BLASTS	160570.500	-1.284	0.199
PERSON-TO-PERSON INTERACTION	163871.000	-0.573	0.566
TV ADVERTS	159337.000	-1.427	0.154
RADIO ANNOUNCEMENTS IN MY LOCAL DIALECTS	162464.000	-0.813	0.416
ROAD SHOWS IN OUR LOCAL AREA	165720.500	-0.129	0.897
NEWSLETTER	162764.000	-1.186	0.235
NEWSPAPER ADVERTS	158033.500	-2.628	0.009
CLASSROOM WORKSHOPS	161185.000	-2.023	0.043
E-MAIL	161432.000	-1.401	0.161
WEB-BASED TRAINING	165908.000	-0.237	0.812

Questionnaire Questions	Mann-Whitney U Test	Z	Asymp. Sig. (2-tailed)
ON-LINE DISCUSSION	163248.000	-0.901	0.368
VIDEO-BASED METHODS	159628.000	-2.543	0.011
Do you keep Personally identifiable information (e.g. your name, bank account number etc.) on your phone?	161512.000	-1.046	0.295
Do you use your phone to access the internet i.e., Facebook, Twitter, Yahoo mail, google etc.?	162161.000	-1.244	0.214
Do you enable location services on your phone?	161055.500	-1.136	0.256
Have you ever downloaded applications and documents from the internet unintentionally or unknowingly?	157755.000	-1.802	0.071
To what extent do you trust the safety of websites you normally access through your phone?	160371.000	-1.134	0.257
Does your phone have an anti-virus program?	149034.500	-3.023	0.003
To what extent are you concerned that some files you download might collect some data from your phone without your knowledge?	152287.500	-0.699	0.485
Are you aware of any security risks associated with using mobile devices?	153635.500	-2.789	0.005
Are you aware you can disable location settings on your phone?	155836.000	-2.533	0.011
Do you know how to change settings/location services on your phone?	158889.000	-1.959	0.050
Do you think information/ data in your phone is important?	160237.000	-1.937	0.053
Have you ever heard of mobile security?	152721.000	-3.153	0.002
Do you know your roles and responsibilities in ensuring secure mobile financial service?	149355.000	-3.739	0.000
Do you have an idea of any ‘social engineering’ tricks for mobile devices or what it means?	163023.000	-0.728	0.467
To what extent do you think you can identify a mobile money hoax (scam) i.e. someone asking you to pay some money to get a prize or posing as a friend and that they are stuck and needs some money?	147970.500	-1.878	0.060
Have you encountered a phishing attack (i.e., someone asking for your MPESA PIN, National ID etc.?	156381.000	-2.194	0.028

Questionnaire Questions	Mann-Whitney U Test	Z	Asymp. Sig. (2-tailed)
Have you had/experienced a vishing attack i.e., someone asking you to call them to claim some money that you have won or someone sending you a message with instructions on how to claim some money you have won?	160445.000	-1.371	0.170
If YES in 45 above, how did you respond?	119140.500	-1.113	0.266
Do you think mobile money security awareness is a challenge that needs to be addressed?	164736.000	-0.576	0.565
Are you aware of any laws governing mobile security in Kenya?	147471.000	-3.880	0.000
Do you think there is a need to have a mobile security education training and awareness in Kenya?	161050.000	-1.568	0.117
If yes in 49 above, on a scale of 0-5(0- I don't know, 1-least priority, 5-high priority), how would you want the following information security concepts be considered for training and awareness? Physical protection of mobile devices	152614.500	-2.535	0.011
Vulnerabilities/password confidentiality	162213.500	-0.752	0.452
Emerging threat and detection (Phishing and vishing schemes)?	157553.500	-1.616	0.106
MFS fraud incident early detection	164944.500	-0.293	0.769
Damage/loss caused by use of mobile money use, failure, malfunction, interruption or unavailability of the mobile financial system	164846.000	-0.307	0.759
Strong security password setup	159053.000	-1.275	0.202
mobile money risks (theft of phone, money sent to wrong number, pin leakage to another person, fake money from agent, fake transaction detections	165105.000	-0.268	0.788

Source: Compiled by the Researcher

Based on the Mann-Whitney U test results presented in Table 5.3, the following interpretations can be made:

Age: There is a statistically significant difference (U = 150227.500, Z = -3.115, p = 0.002) in responses related to age concerning mobile money security awareness.

Ownership of a Mobile Phone: Participants who differ in the duration of owning a mobile phone also show a statistically significant difference (U = 149359.000, Z = -3.228, p = 0.001) in their attitudes towards mobile money security.

Security Measures Awareness: Awareness about phone security measures such as password and PIN usage (U = 151532.000, Z = -3.819, p = 0.000) significantly influences attitudes towards mobile money security.

Awareness of Mobile Security Laws: Participants aware of mobile security laws in Kenya (U = 147471.000, Z = -3.880, p = 0.000) show significantly different perceptions regarding mobile money security compared to those unaware.

Awareness of Mobile Security Education Needs: Individuals recognizing the need for mobile security education and awareness (U = 161050.000, Z = -1.568, p = 0.117) demonstrate varied priorities in different aspects of information security training.

These findings suggest that demographic factors such as age and duration of mobile phone ownership, as well as awareness of security measures and legal frameworks, significantly influence perceptions and behaviours related to mobile money security among the study participants. These results are crucial for informing targeted educational interventions and policy initiatives aimed at enhancing mobile money security awareness and practices.

5.3.1. Gender of Mobile Financial Users

The figure 5.1 shows the gender composition of the participants in this study.

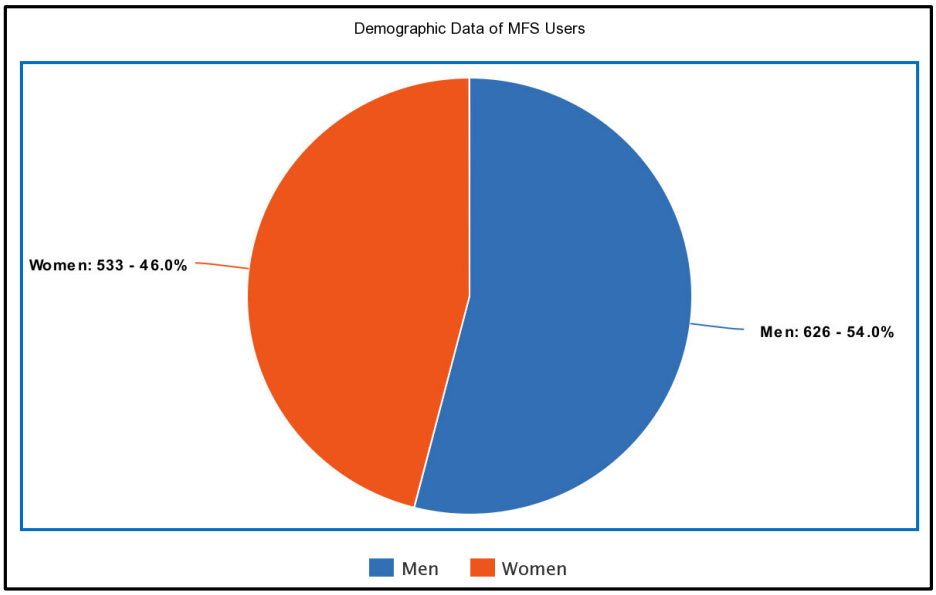


Figure 5.1 Gender Representation of Mobile Money Users

Source: Compiled by the Researcher

The study involved a total of 626 male mobile money users who participated in the research, comprising 54% of the sample, outnumbering females by 9%. Female participants numbered 533, making up approximately 46% of the total sample.

Gender by Place of Residence

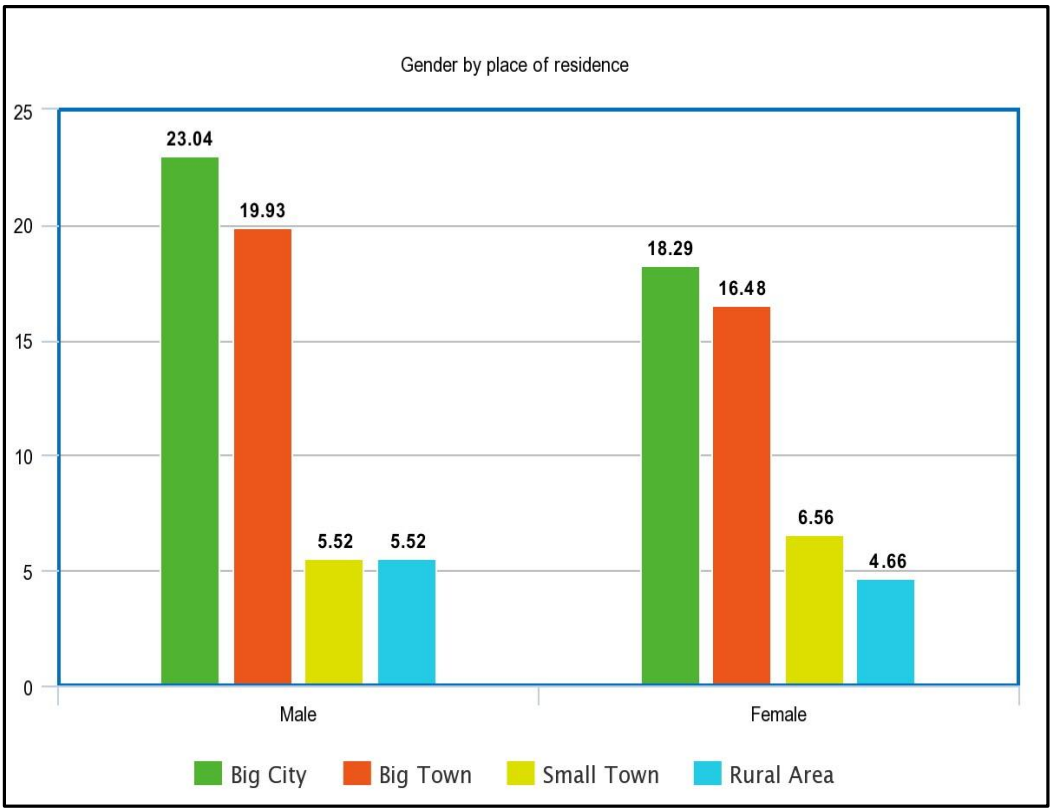


Figure 5.2 Gender by Place of Residence

Source: Compiled by the Researcher

Of the male participants, 23% lived in a big city, compared to 18% of the female participants. Those who lived in big towns constituted 20% and 16% for males and females, respectively. Among the male participants, 64 resided in a small town, as did 76 of their female counterparts. In total, 49% of the male participants resided in urban areas, including big cities, big towns, or small towns, with only 6% of the males living in rural areas. The number of females in urban areas accounted for 41% of their cumulative 46%.

The influence of gender on cybersecurity behaviour among MFS users will also be examined in the subsequent sections.

Table 5.4 Cross-tabulation Showing Relationship Between Gender and Presence of Passwords/Security Codes for Locking

		Gender	
		Male	**Female**
		Column N %	**Column N %**
Does your mobile phone have any password/security codes for locking?	Yes	83.9%	74.1%
	No	7.7%	15.9%
	I don't know	8.5%	9.9%

Source: Compiled by the Researcher

The data illustrates the relationship between gender and the presence of passwords or security codes for locking mobile phones. The study reveals that among male respondents, 83.9% reported using a password or security code for locking their mobile phones, while 7.7% indicated they did not use any such security measure, and 8.5% were uncertain. In contrast, among female respondents, 74.1% reported using a password or security code, 15.9% stated they did not, and 9.9% were unsure.

This analysis highlights a notable difference in the adoption of security measures between genders, with a higher percentage of males than females using passwords or security codes on their mobile phones. The findings suggest that gender may play a role in security behaviours related to mobile device use, influencing the likelihood of employing protective measures such as passwords or security codes.

5.4. CORRELATION

Table 5.5 Correlation Between Bender and whether the Phone has any Password/Security codes for Locking

		Gender	Does your mobile phone have any password/security codes for locking?
Gender	Pearson Correlation	1	.089**
	Sig. (2-tailed)		.002
	N	1159	1159
Does your mobile phone have any password/security codes for locking?	Pearson Correlation	.089**	1
	Sig. (2-tailed)	.002	
	N	1159	1159

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Compiled by the Researcher

A weak positive correlation (r = 0.089, p = 0.002) was observed between gender and the presence of a password or security code on mobile phones, indicating statistical significance. This suggests that the likelihood of having a password or security code on mobile phones varies slightly between genders.

The data indicate that both males and females tend to use passwords or security codes to lock their phones, with males exhibiting a slightly higher tendency. This relationship is supported by a significant p-value of 0.002, suggesting a gender-based association with phone security practices.

Overall, these findings imply that gender may play a minor role in determining the likelihood of using a password or security code on mobile phones. However, the correlation strength (r = 0.089) suggests that gender alone is not a robust predictor of phone security practices.

Table 5.6 Correlation Between Gender and Extent of Trust for the Platform

			To what extent do you trust the mobile platform when undertaking a financial transaction?					
			Very small extent	Small extent	Never	Large extent	Very large extent	Total
Gender	Male	Count	32	122	50	274	148	626
		% within Gender	5.1%	19.5%	8.0%	43.8%	23.6%	100.0%
	Female	Count	32	117	49	215	120	533
		% within Gender	6.0%	22.0%	9.2%	40.3%	22.5%	100.0%
Total		Count	64	239	99	489	268	1159
		% of Total	5.5%	20.6%	8.5%	42.2%	23.1%	100.0%

Source: Compiled by the Researcher

The table presents the counts and percentages of males and females who trust mobile financial platforms to varying extents. A higher percentage of males (67.4%) report trusting the mobile financial platform to a large or very large extent compared to females (62.8%). Conversely, a higher percentage of females (37.2%) report a very small extent, small extent, or never trusting the platform compared to males (32.6%). The analysis reveals that both genders exhibit similar patterns of trust in mobile financial services platforms, with females demonstrating slightly higher levels of trust compared to males. This finding is crucial for stakeholders in the financial technology sector, as it implies that trust-building measures and strategies need not be gender-specific but rather can be designed to address the broader user base uniformly.

5.4.1. Age Range of Mobile Money Users

The youth aged between 18–25 constituted a large percentage of the participants, accounting for almost half the sample at 43%, as presented in Figure 5.3. The 18–25 age group was the modal age group. Participants aged between 25–40 comprised 33% of the sample, while those between 41–50 years accounted for 14.5%. Participants between 51–60 represented 6.7% of the sample, and those aged 61 years and above accounted for 2.5%.

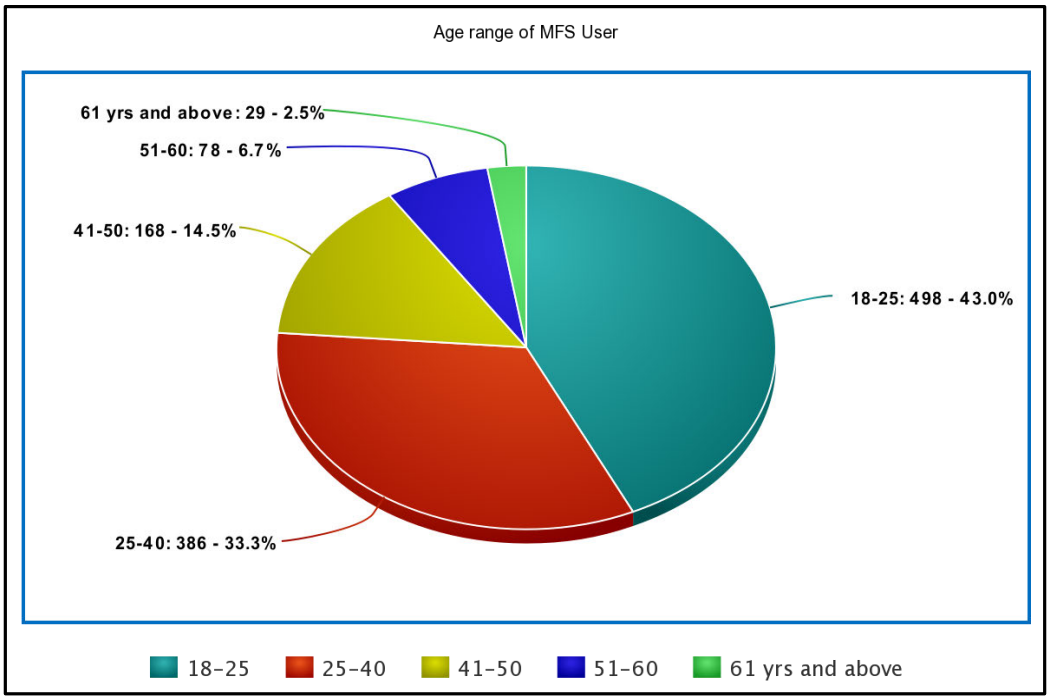


Figure 5.3 Age Range of Mobile Money Users

Source: Compiled by the Researcher

Age Range of Mobile Money Users as per area of residence

Table 5.7 Age Range of Mobile Money Users as Per Area of Residence

Age Range	Total	Big City	Big Town	Small Town	Rural Area
18–25	498	206	181	60	51
25–40	386	159	141	47	39
41–50	168	69	61	20	18
51–60	78	32	28	10	8
61 years and above	29	11	11	4	3
Total	1159	477	422	141	119

Source: Compiled by the Researcher

As per Table 5.8, it can be concluded that most mobile phone users reside in big cities and large towns. This is evidenced by the age range distribution. The age range (18–25) primarily resides in big cities and large towns, and this same age range is the most prevalent according to this survey. In general, all the age ranges prefer settling in a big city or town, followed by a small town, and then rural areas.

Table 5.8 Cross-Tabulation between Age and Having a Phone Security Code

Age Range	Does your mobile phone have any password/security codes for locking?			Total
	Yes	No	I Don't Know	
18–25	423	48	27	498
25–40	312	37	37	386
41–50	125	25	18	168
51–60	47	16	15	78
61 years and above	13	7	9	29
Total	920	133	106	1159

Source: Compiled by the Researcher

The data were analysed to investigate the relationship between age and the use of phone security codes. It was observed that younger age groups, particularly those between 18–25 and 25–40 years, exhibit higher rates of using phone security codes compared to older age groups. Conversely, older respondents, especially those aged 61 years and above, demonstrate lower adoption rates of phone security codes. These findings highlight the need for targeted mobile security awareness campaigns tailored to different age demographics. Younger individuals may benefit from campaigns emphasizing the importance and methods of implementing phone security codes, while strategies for older demographics could focus on addressing barriers to adoption and promoting ease of use. This analysis contributes valuable insights into understanding age-related patterns in mobile security behaviour, crucial for developing effective policies and awareness initiatives in mobile security management.

5.4.1.1. Influence of Age on Protection behaviour of the MFS users

Table 5.9 Age and the Ability to Protect One's Digital Device

			Age				
			18-25	**25-40**	**41-50**	**51-60**	**Above 61 years**
Protect	Do you know how to physically secure your phone i.e., put auto lock password on and require password to unlock without help?	Yes	44.0%	34.3%	14.4%	5.5%	1.7%
		No	34.6%	25.2%	15.0%	16.5%	8.7%
	Does your mobile phone have any password/security codes for locking?	Yes	46.0%	33.9%	13.6%	5.1%	1.4%
		No	36.1%	27.8%	18.8%	12.0%	5.3%
		I don't know	25.5%	34.9%	17.0%	14.2%	8.5%

Source: Compiled by the Researcher

The data suggest a varying level of awareness and practice in securing mobile phones across different age groups:

Younger Age Groups (18-25): Show a higher propensity to know and implement phone security measures such as using passwords. This may reflect greater familiarity with technology and digital security practices among younger demographics.

Older Age Groups: Exhibit mixed responses, with a significant portion unsure about their phone security status. This underscores potential gaps in awareness or usability concerns regarding security features among older users.

Understanding these age-related variations in mobile phone security practices is crucial for developing targeted educational programs and user-friendly security interfaces. This analysis contributes to the broader discourse on cybersecurity education and user behaviour, highlighting areas for intervention to enhance digital security practices across all age groups.

5.4.1.2. Influence of Age on the ability to detect by MFS users

Table 5.4 Relationship Between Age and the Ability to Detect a Cybersecurity Attack

			Age				
			18-25	**25-40**	**41-50**	**51-60**	**Above 61 years**
Detect	To what extent do you think you can recognize if your phone has been hacked?	Never	41.7%	33.3%	14.1%	5.7%	5.2%
		Rarely	43.4%	32.0%	14.3%	6.8%	3.4%
		Sometimes	54.8%	29.4%	11.0%	3.5%	1.3%
		Most of the time	38.8%	36.7%	12.9%	10.1%	1.4%
		Always	31.9%	38.3%	20.7%	9.0%	0.0%

Source: Compiled by the Researcher

The findings suggest that younger age groups, particularly those between 18-40 years, generally express higher confidence in detecting cybersecurity attacks on their phones compared to older age groups. Conversely, older adults, especially those above 61 years, appear to have less confidence in their ability to detect such attacks. This data underscores the importance of age as a factor influencing perceived cybersecurity awareness and readiness, with implications for cybersecurity education and awareness programs targeted at different age demographics.

5.4.2. Highest Level of Education

Table 5.12 demonstrates that a significant portion of respondents held bachelor's degrees, at 26.5%, while the fewest possessed master's degrees, accounting for 6.6% of the participants. This section includes a discussion on the impact of level of education of MFS users on cybersecurity behaviour.

Table 5.5 What is Your Highest Level of Education?

Level of Education	Frequency	%	Cumulative %
No formal education	72	6.2	6.2
KCPE certificate	149	12.9	19.1
KCSE Certificate	252	21.7	40.8
Artisan/Craft Certificate	99	8.5	49.3
Diploma	215	18.6	67.9
Bachelor's Degree	307	26.5	94.4
Master's Degree	65	6.6	100.0

Source: Compiled by the Researcher

Table 5.6 Cross-Tabulation of Education and Ability to Recognize if One's Phone Has Been Hacked

		Level of Education?						
		No Formal Education	KCPE Certificate	KCSE Certificate	Artisan / Craft Certificate	Diploma	Bachelor's Degree	Master's Degree
Recognize if phone has been hacked?	Never	22.2%	20.8%	20.6%	23.2%	11.2%	11.7%	15.4%
	Rarely	51.4%	36.9%	31.7%	38.4%	38.1%	30.6%	40.0%
	Sometimes	9.7%	12.8%	24.2%	14.1%	18.6%	24.1%	20.0%
	Most of the time	11.1%	4.0%	11.1%	4.0%	13.5%	17.6%	15.4%
	Always	5.6%	25.5%	12.3%	20.2%	18.6%	16.0%	9.2%

Source: Compiled by the Researcher

The table shows the relationship between the level of education and the extent to which the MFS subscribers can recognize if their phones have been hacked. Across all educational levels, individuals who reported 'rarely' recognizing if their phone has been hacked represented the highest proportion. Specifically, those with No formal education reported 51.4%, KCPE Certificate holders 36.9%, KCSE Certificate holders 31.7%, Artisan/Craft Certificate holders 38.4%, Diploma holders 38.1%, Bachelor's Degree holders 30.6%, and Master's Degree

holders 40.0%. The analysis highlights a potential correlation between higher levels of education and a lower frequency of recognizing if one's phone has been hacked, particularly evident in the lower percentages of those reporting 'never' being aware of such occurrences among Bachelor's and Master's Degree holders.

Table 5.7 Level of Education and Dependence of Someone to Help with Completing Mobile Money Transaction

		How often do you seek assistance from people with your phone to carry out MPESA/Mobile money transactions?				
		Always	**Many times**	**Once**	**Never**	**Total**
What is your highest level of education?	No Formal Education	10	11	11	40	72
	KCPE Certificate	10	11	36	92	149
	KCSE Certificate	23	18	52	159	252
	Artisan / Craft Certificate	4	10	37	48	99
	Diploma	7	9	52	147	215
	Bachelor's Degree	13	19	39	236	307
	Master's Degree	4	1	8	52	65
Total		71	79	235	774	1159

Source: Compiled by the Researcher

The data reveals varying levels of dependence on assistance for mobile money transactions across educational levels. Higher frequencies of seeking assistance ('Always' and 'Many Times') are observed in lower education categories and decrease as education level increases.

Individuals with lower education levels, such as those with No Formal Education or up to KCPE and KCSE Certificates, show higher frequencies of seeking assistance compared to those with higher education levels such as Bachelor's and Master's Degrees.

This pattern suggests that higher levels of education may correlate with reduced dependency on others for mobile money transactions. Factors such as familiarity with technology and financial literacy, which typically increase with higher education, may contribute to this trend.

Table 5.8 Cross-Tabulation Between Level of Education and Having Password for Phone Locking

		Does your mobile phone have any password/security codes for locking?			
		Yes	**No**	**I Don't Know**	**Total**
What is your highest level of education?	No Formal Education	34	19	19	72
	KCPE Certificate	105	24	20	149
	KCSE Certificate	213	20	19	252
	Artisan/Craft Certificate	77	18	4	99
	Diploma	165	23	27	215
	Bachelors' Degree	275	22	10	307
	Masters' Degree	51	7	7	65
Total		920	133	106	1159

Source: Compiled by the Researcher

Table 5.15 summarizes responses regarding the presence of a Password or Security Code on mobile phones across different levels of education. The data indicate varying levels of adoption of phone security measures among respondents with different educational backgrounds. Among respondents with No Formal Education, 34 individuals reported having a Password for Phone Locking, while 19 did not, and 19 were unsure. Similar patterns are observed across other educational categories, with higher counts of individuals having a Password as educational attainment increases. For instance, among those with a Bachelors' Degree, 275 respondents reported having a Password, 22 did not, and 10 were unsure. The data show a consistent trend where higher educational levels generally correspond to a higher likelihood of having a Password for Phone Locking.

Overall, the table underscores the correlation between educational achievement and the adoption of digital security practices, highlighting a need for targeted interventions to promote awareness and implementation of cybersecurity measures across diverse educational backgrounds. This analysis provides valuable insights into the relationship between education and personal cybersecurity behaviours, which is critical for informing policies and educational strategies aimed at enhancing digital security awareness and practices among the population.

Table 5.9 Influence of Level of Education on the Ability to Protect

			Level of Education						
			No Formal Education	KCPE Certificate	KCSE Certificate	Artisan / Craft Certificate	Diploma	Bachelor's Degree	Master's Degree
Protect	Do you know how to physically secure your phone i.e., Put auto lock password on and require password to unlock without help?	Yes	4.1%	11.5%	22.5%	9.1%	19.0%	28.2%	5.6%
		No	23.6%	23.6%	15.7%	3.9%	15.0%	12.6%	5.5%

Source: Compiled by the Researcher

The data suggests a positive correlation between higher levels of education and the ability to secure phones. Specifically, higher percentages of individuals with Bachelor's and Master's degrees demonstrate knowledge of phone security compared to those with lower educational qualifications. Individuals with KCSE Certificate, Artisan/Craft Certificate, Diploma, Bachelor's Degree, and Master's Degree show varying levels of knowledge in phone security, generally indicating that formal education might contribute positively to security awareness.

Table 5.10 Influence of Level of Education on the Ability to Detect

			Level of Education						
			No Formal Education	KCPE Certificate	KCSE Certificate	Artisan / Craft Certificate	Diploma	Bachelor's Degree	Master's Degree
Detect	To what extent do you think you can recognize if your phone has been hacked?	Never	8.3%	16.1%	27.1%	12.0%	12.5%	18.8%	5.2%
		Rarely	9.0%	13.3%	19.4%	9.2%	19.9%	22.8%	6.3%
		Sometimes	3.1%	8.3%	26.8%	6.1%	17.5%	32.5%	5.7%
		Most of the time	5.8%	4.3%	20.1%	2.9%	20.9%	38.8%	7.2%
		Always	2.1%	20.2%	16.5%	10.6%	21.3%	26.1%	3.2%

Source: Compiled by the Researcher

The data suggests that individuals with higher education levels, particularly those with a Bachelor's Degree and Diploma, exhibit greater confidence and ability in detecting phone hacks. In contrast, those with lower levels of education, such as no formal education or only a KCPE Certificate, show lower confidence in recognizing potential phone hacks. This trend

indicates a potential correlation between higher education levels and increased digital literacy or awareness, which may contribute to better cybersecurity vigilance.

Table 5.11 Influence of Level of Education on the Ability to Recover from a Cyber-Attack

			Level of Education						
			No Formal Education	**KCPE Certificate**	**KCSE Certificate**	**Artisan / Craft Certificate**	**Diploma**	**Bachelor's Degree**	**Master's Degree**
Recover	How did you report if you have lost money via MPESA / mobile banking?	Did not answer	4.5%	7.2%	21.3%	6.0%	15.6%	37.8%	7.5%
		Police	7.7%	18.3%	26.6%	8.9%	23.1%	13.6%	1.8%
		Service provider	6.1%	14.0%	20.7%	9.8%	19.8%	24.6%	5.0%
		I just kept quiet	9.5%	15.5%	20.7%	9.5%	14.7%	21.6%	8.6%

Source: Compiled by the Researcher

The data indicate that individuals with a KCSE certificate reported the highest incidence of contacting the police, at 26.6%. This was followed by those with a KCPE certificate (18.3%) and a diploma (23.1%). In contrast, the lowest reporting rate to the police was observed among individuals with a master's degree, at 1.8%. This trend suggests that individuals with lower educational qualifications may have a higher propensity to involve law enforcement, possibly due to a lack of alternative resources or knowledge. Reporting to the service provider was most prevalent among individuals with a bachelor's degree (24.6%), followed by those with a diploma (19.8%) and a KCSE certificate (20.7%). The lowest rate was observed among those with a master's degree, at 5.0%. This pattern indicates that individuals with higher education levels may prefer to seek assistance from service providers, potentially due to a better understanding of available support channels.

The analysis reveals significant variations in recovery strategies based on the level of education. Individuals with higher education levels tend to refrain from answering and prefer contacting service providers, whereas those with lower education levels are more inclined to report to the police. These findings highlight the need for tailored support and education strategies to ensure that all individuals, regardless of their educational background, have access to appropriate recovery mechanisms in case of financial loss via MPESA/mobile banking.

5.4.3. Main Area of Residence

Table 5.12 Mobile Money Users by Residence

Area of Residence	Frequency	%	Cumulative %
Big City	479	41.3	41.3
Big Town	422	36.4	77.7
Small Town	140	12.1	89.8
Rural Area	118	10.2	100.0
Total	1159	100.0	

Source: Compiled by the Researcher

As detailed in Table 5.19, a significant percentage of the participants, approximately 78% of the total sample, reside in big cities or large towns. The smaller figures for those from small towns or rural areas confirm that much of the survey was administered to people in urban areas.

Table 5.13 Showing Cross-Tabulation of Place of Residence and Recognize If Your Phone Has Been Hacked

		Place of Residence			
			Big Town	Small Town	Rural Area
		Column N %	Column N %	Column N %	Column N %
Recognize hacking?	Yes	83.3%	79.6%	77.1%	65.3%
	No	11.7%	9.2%	8.6%	22.0%
	I don't know	5.0%	11.1%	14.3%	12.7%

Source: Compiled by the Researcher

The analysis indicates a noticeable trend where individuals residing in big towns demonstrate the highest ability to recognize if their phone has been hacked, followed closely by those in small towns. Conversely, the ability to recognize hacking decreases slightly in rural areas. This trend may suggest that urbanization and the associated exposure to digital literacy and cybersecurity awareness play a critical role in the ability to recognize cyber threats.

The overall population data reflects a broader perspective, where approximately two-thirds of respondents possess the ability to recognize hacking. However, the combined category also reveals a higher percentage of individuals who cannot recognize hacking and those who are

uncertain, compared to the segmented data. This suggests that targeted awareness programs might be beneficial in enhancing the overall population's ability to detect cybersecurity threats, especially in less urbanized areas.

Table 5.14 Correlation Between Place of Residence and If MFS Users Can Recognize If Their Phones Have Been Hacked

		Place of Residence	Recognize Hacking?
Place of residence	Pearson Correlation	1	.129**
	Sig. (2-tailed)		.000
	N	1159	1159

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Compiled by the Researcher

A Pearson Correlation analysis was conducted on a sample of 1159 MFS users. The variables analysed were the place of residence and the recognition of phone hacking incidents. The significance of the correlation was evaluated using a two-tailed test with a significance level of 0.05. The Pearson Correlation coefficient for the relationship between place of residence and the recognition of phone hacking was found to be r=0.129r = 0.129r=0.129, with a significance level of p=0.000p = 0.000p=0.000. This indicates a weak but statistically significant positive correlation between the two variables.

The positive correlation suggests that there is a relationship between the place of residence and the ability of MFS users to recognize if their phones have been hacked. However, the correlation coefficient value of 0.129 indicates that the strength of this relationship is weak. Despite the weak correlation, the statistical significance ($p < 0.05$) implies that the relationship is unlikely to be due to random chance. It can be concluded that the place of residence has a weak yet significant impact on the recognition of phone hacking among MFS users. This finding suggests that geographical factors may play a role in cybersecurity awareness and detection capabilities.

Table 5.15 Cross-Tabulation Between Place of Residence and the Extent that MFS Users Are Concerned About Downloading Files That Might Collect Some Data from Their Phones Without Their Knowledge

		Place of Residence			
		Big City	**Big Town**	**Small Town**	**Rural Area**
		Column N %	**Column N %**	**Column N %**	**Column N %**
The extent concerned about downloading files might collect some data with your knowledge	Very small extent	5.6%	3.6%	8.8%	5.4%
	Small extent	23.4%	31.8%	28.5%	34.2%
	Never	25.3%	20.1%	25.5%	22.5%
	Large extent	24.5%	26.7%	27.7%	18.9%
	Very large extent	21.2%	17.7%	9.5%	18.9%

Source: Compiled by the Researcher

The analysis reveals variation in the extent of concern about downloading files that might collect data from users' phones based on their place of residence. Users in rural areas and big towns tend to show higher percentages of concern to a small extent, while users in big cities and small towns exhibit more significant concern either to a very large extent or very small extent. This information is crucial for understanding the different levels of awareness and concern among MFS users in various residential settings, which can inform targeted educational and security measures.

Table 5.16 Correlation Between the Place of Residence and the Extent that MFS Users are Concerned that Some Files Downloaded Might Collect Some Data from Your Phone Without Their Knowledge

		Place of Residence	**Downloading Files Without Knowledge?**
Place of residence	Pearson Correlation	1	-.077*
	Sig. (2-tailed)		.010
	N	1159	1122
	N	1159	1122
Downloading files without knowledge?	Pearson Correlation	-.077*	1
	Sig. (2-tailed)	.010	

N	1122	1122

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Compiled by the Researcher

The Pearson correlation coefficient between the place of residence and the concern about downloading files is indicated as -0.077, with a significance level (p-value) of 0.010. This correlation is statistically significant, as the p-value is less than the conventional threshold of 0.05. The significance (2-tailed) value of 0.010 confirms that there is a statistically significant relationship between the two variables. This indicates that the observed correlation is unlikely to have occurred by random chance. Despite the weak strength of the correlation, its statistical significance implies that place of residence does have a minor influence on the level of concern regarding downloading files that might surreptitiously collect data.

The analysis reveals a weak but statistically significant negative correlation between the place of residence and the concern about downloading files that might collect data without users' knowledge. This finding suggests that there are minor variations in concerns based on the place of residence, with residents of certain areas being slightly less concerned about potential data collection through downloaded files.

Influence of the place of residence on one's ability to protect

Table 5.17 Cross-Tabulation of Place of Residence and Ability to Protect One's Digital Device

			Place of Residence			
			Big City	**Big Town**	**Small Town**	**Rural Area**
Protect	Do you know how to physically secure your phone i.e., Put auto lock password on and require password to unlock without help?	Yes	41.8%	36.8%	11.8%	9.6%
		No	37.8%	33.1%	14.2%	15.0%
	Have you shared your phone with someone to help you with a transaction?	Yes	41.7%	34.1%	11.1%	13.1%
		No	41.1%	37.8%	12.7%	8.4%

Source: Compiled by the Researcher

From the data, it can be observed that residents of big cities and big towns exhibit higher levels of knowledge regarding the physical security of their phones compared to residents of small towns and rural areas. The percentage of individuals who know how to secure their phones

without assistance is highest in big cities (41.8%), followed by big towns (36.8%). In contrast, small towns (11.8%) and rural areas (9.6%) show significantly lower percentages. The trend is consistent with the pattern of urbanization, suggesting that urban residents have greater access to information and resources related to digital security.

The analysis indicates a clear correlation between the place of residence and the ability to protect one's digital device. Urban residents, particularly those in big cities and towns, demonstrate higher knowledge of phone security measures and a more balanced approach to sharing phones for transactional assistance. In contrast, residents of small towns and rural areas show lower knowledge of physical security and a lower propensity to share their phones. This disparity highlights the need for targeted educational initiatives to improve digital security awareness and practices in less urbanized areas.

Influence of the place of residence on one's ability to respond

Table 5.18 Cross-Tabulation Between and One's Ability to Respond to a Cyber-Attack

			Place of Residence			
			Big City	**Big Town**	**Small Town**	**Rural Area**
Respond	How did you report if you have lost money via MPESA/mobile banking?	Did not answer	50.8%	29.1%	12.3%	7.8%
		Police	46.7%	32.5%	10.7%	10.1%
		Service provider	36.0%	40.9%	11.6%	11.5%
		I just kept quiet	31.0%	42.2%	15.5%	11.2%

Source: Compiled by the Researcher

Big cities and big towns show higher percentages of individuals reporting incidents to the police, with 46.7% and 32.5%, respectively. The percentages drop significantly in small towns (10.7%) and rural areas (10.1%). This indicates that urban residents are more likely to involve law enforcement in such incidents, possibly due to better access to police services and a higher trust in formal institutions.

A higher percentage of individuals in big towns reported incidents to their service provider (40.9%), compared to big cities (36.0%). Small towns and rural areas reported lower percentages, at 11.6% and 11.5%, respectively. The preference for reporting to service providers in big towns may reflect a higher reliance on these entities for resolving issues related to mobile banking.

The highest percentage of individuals who chose to keep quiet about the incident was observed in big towns (42.2%), followed by big cities (31.0%). Small towns (15.5%) and rural areas (11.2%) reported lower percentages. This trend suggests a significant number of urban residents might prefer not to disclose such incidents, potentially due to fear of stigma, lack of confidence in recovery mechanisms, or other personal reasons.

The analysis demonstrates that the place of residence significantly influences how individuals report and recover from cybersecurity incidents involving mobile banking. Urban residents, particularly those in big cities and towns, show a higher propensity to report to the police and service providers but also a notable tendency to either not answer or keep quiet about such incidents. In contrast, residents of small towns and rural areas exhibit lower reporting rates, indicating potential barriers to accessing or trusting formal recovery mechanisms. These findings underscore the need for targeted interventions to enhance cybersecurity awareness and reporting mechanisms, especially in less urbanized areas.

5.4.4. Years of Owning a Phone

Figure 5.4 graphs the distribution of mobile financial users by years of owning a phone.

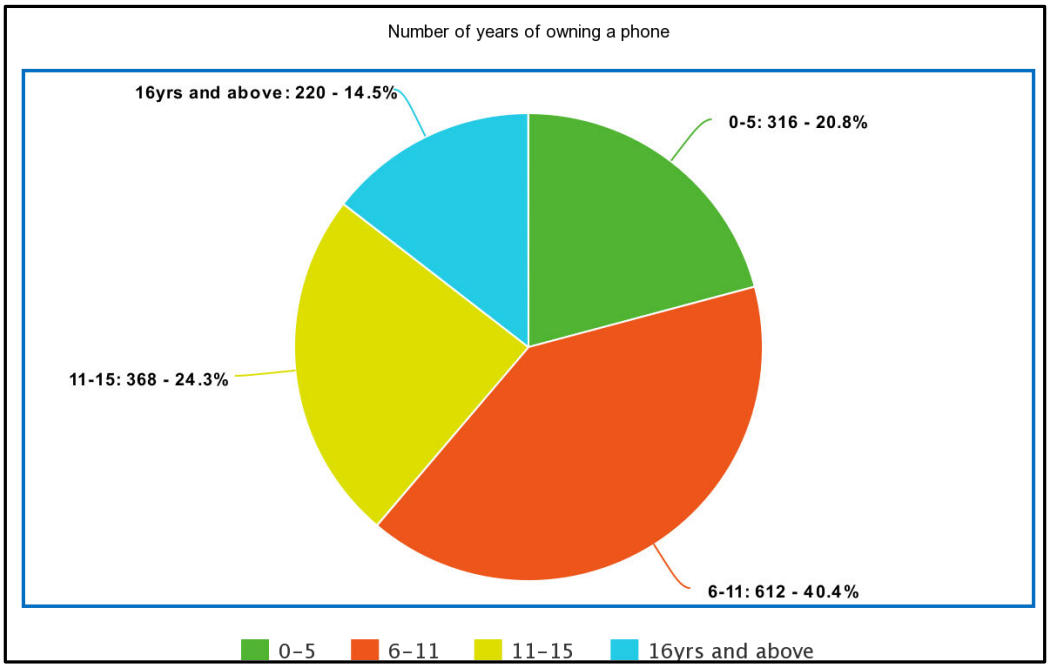


Figure 5.4 Years of Owning a Mobile Phone

Source: Compiled by the Researcher

Respondents who had owned mobile phones for 6 to 11 years accounted for 40% of the total sample. This was followed by those who owned their phones for between 11–15 years at 24%.

Those who had owned a phone for 0–5 years were also represented, while 15% had owned a mobile phone for 16 years and above.

Table 5.19 Correlation Between Years of Owning a Phone and if the MFS User Shared Their Phone with Someone to Help with a Financial Transaction

		Years of Owning a Phone	Some Helped with a transaction?
Years of owning a phone	Pearson Correlation	1	-.132**
	Sig. (2-tailed)		.000
	N	1159	1159
"Someone helped with a transaction?"	Pearson Correlation	-.132**	1
	Sig. (2-tailed)	.000	
	N	1159	1159

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: Compiled by the Researcher

The significance (Sig. 2-tailed) value associated with this correlation is 0.000, which is less than the conventional threshold of 0.05. This indicates that the observed correlation is statistically significant, suggesting that the relationship between the years of owning a phone and the likelihood of sharing the phone for financial transactions is unlikely to be due to random chance. The negative correlation implies that as the number of years of owning a phone increases, the likelihood of an individual sharing their phone to help with a financial transaction slightly decreases. This relationship, although weak, is statistically significant and could suggest that more experienced phone users may be more cautious about sharing

their devices for financial activities. This caution could be attributed to increased awareness of security risks or a higher degree of personal responsibility associated with longer phone ownership. These findings contribute to understanding user behaviour in mobile financial services and may inform strategies to enhance security and user trust in these services.

Table 5.20 Correlation Between Years of Owning Phone and Confidence in Using Mobile Money

			Age	**For how long you have owned a mobile phone?**	**What is your highest level of education?**	**On a scale of 1 to 5, how would you rate your confidence when using your phone to perform MPESA/Mobile money transactions without requiring help from someone else?**
Spearman's rho	Age	Correlation Coefficient	1.000	.422**	-.136**	-.092**
		Sig. (2-tailed)	.	.000	.001	.002
	"For how long have you owned a mobile phone?"	Correlation Coefficient	.422**	1.000	.034	.201**
		Sig. (2-tailed)	.000	.	.249	.001
	"What is your highest level of education?"	Correlation Coefficient	-.136**	.034	1.000	.241**
		Sig. (2-tailed)	.000	.250	.	.000
	On a scale of 1 to 5, how would you rate your confidence when using your phone to perform MPESA/Mobile money transactions without requiring help from someone else?	Correlation Coefficient	-.092**	.201**	.241**	1.000
		Sig. (2-tailed)	.002	.000	.000	.

Source: Compiled by the Researcher

In examining the correlation between Years of Owning Phone and Confidence in Using Mobile Money, the data reveals several significant findings.

Firstly, there is a moderately positive correlation (rho = 0.422, $p < 0.001$) between the length of time individuals have owned their mobile phones and their confidence in using mobile money services independently. This suggests that individuals who have owned their phones for longer periods tend to exhibit higher levels of confidence in conducting MPESA/Mobile money transactions without assistance.

Secondly, the correlation between Years of Owning Phone and Education Level is negligible (rho = 0.034, p = 0.249), indicating no significant relationship between these variables.

Lastly, there is a weak negative correlation (rho = -0.092, p = 0.002) between Age and Confidence in Using Mobile Money, indicating that older individuals may exhibit slightly lower confidence in using mobile money services independently compared to younger individuals.

Overall, the data suggests that the duration of phone ownership plays a significant role in shaping individuals' confidence levels in using mobile money services independently, while age and education level exhibit weaker or negligible associations with confidence in this context. These findings underscore the importance of familiarity with mobile technology in enhancing confidence in mobile money usage.

Correlation between the variables

Table 5.21 The Relationship Between Demographic Data and Attributes Determining Secure Behaviour Among Users of Mobile Financial Services

		Gender	Age	Level of Education	Place of Residence	Protect	Detect	Respond	Recover
Gender	Pearson Correlation	1	-.057	-.004	.035	.052	-.043	.022	-.023
	Sig. (2-tailed)		.052	.901	.238	.078	.144	.446	.434
	N	1159	1159	1159	1159	1159	1159	1158	1159

		Gender	Age	Level of Education	Place of Residence	Protect	Detect	Respond	Recover
Age	Pearson Correlation	-.057	1	-.162**	.066*	.129**	-.021	-.062*	.173**
	Sig. (2-tailed)	.052		.000	.025	.000	.476	.034	.000
	N	1159	1159	1159	1159	1159	1159	1158	1159
Level of Education	Pearson Correlation	-.004	-.162**	1	-.131**	-.096**	.139**	.134**	-.106**
	Sig. (2-tailed)	.901	.000		.000	.001	.000	.000	.000
	N	1159	1159	1159	1159	1159	1159	1158	1159
Place of Residence	Pearson Correlation	.035	.066*	-.131**	1	.104**	-.065*	.137**	.109**
	Sig. (2-tailed)	.238	.025	.000		.000	.027	.000	.000
	N	1159	1159	1159	1159	1159	1159	1158	1159
Protect	Pearson Correlation	.052	.129**	-.096**	.104**	1	-.274**	.155**	.023
	Sig. (2-tailed)	.078	.000	.001	.000		.000	.000	.441
	N	1159	1159	1159	1159	1159	1159	1158	1159
Detect	Pearson Correlation	-.043	-.021	.139**	-.065*	-.274**	1	.055	.041
	Sig. (2-tailed)	.144	.476	.000	.027	.000		.063	.161
	N	1159	1159	1159	1159	1159	1159	1158	1159
Respond	Pearson Correlation	.022	-.062*	.134**	.137**	.155**	.055	1	.104**
	Sig. (2-tailed)	.446	.034	.000	.000	.000	.063		.000
	N	1158	1158	1158	1158	1158	1158	1158	1158

		Gender	Age	Level of Education	Place of Residence	Protect	Detect	Respond	Recover
Recover	Pearson Correlation	-.023	.173**	-.106**	.109**	.023	.041	.104**	1
	Sig. (2-tailed)	.434	.000	.000	.000	.441	.161	.000	
	N	1159	1159	1159	1159	1159	1159	1158	1159

Source: Compiled by the Researcher

Place of Residence also plays a role in shaping protective, responsive, and recovery behaviours. Place of Residence correlates positively with Protect (0.1040.1040.104**),** Respond **(**0.1370.1370.137), and Recover (0.1090.1090.109**), indicating that where a person lives can impact their protection, response, and recovery measures. Level of education is positively correlated with Detect (0.1390.1390.139**),** Respond **(**0.1340.1340.134. These suggest that higher education levels are associated with better detection and response capabilities. The analysis reveals intricate relationships between demographic variables (Gender, Age, Level of Education, Place of Residence) and key measures (Protect, Detect, Respond, Recover). Age and Level of Education appear to be particularly influential, with several significant correlations. Notably, protection and detection measures show a strong negative correlation, highlighting a potential area for strategic balancing in interventions.

5.5. AN ANALYSIS OF CYBERSECURITY AWARENESS VARIABLE AMONG MOBILE FINANCIAL SERVICE SUBSCRIBERS

This section addresses the research question concerning the application of constructs derived from the NIST Cybersecurity/Media Pro Adaptive Awareness framework to enhance awareness among users of Mobile Financial Services (MFS). The constructs from both frameworks are introduced, along with their distribution in the questionnaire.

The constructs selected for analysis are drawn from the NIST Cybersecurity and Media Pro Adaptive Awareness frameworks. These frameworks are pivotal in understanding user awareness and behaviour in digital security contexts. The distribution of these constructs within the questionnaire allows for a comprehensive examination of their influence on user awareness levels within the MFS environment.

5.5.1. Distribution of MediaPro Adaptive Awareness Constructs

5.5.1.1. Identify

Table 5.22 Distribution of Identify in the Questionnaire

Identify		Frequency	Percentage (%)
Are you aware that you are not supposed to keep your MPESA PIN/Mobile Bank password as a draft message on your phone?	Yes	983	84.8%
	No	176	15.2%
Have you set your phone to show password/PIN when entering it(so you ca easily know what you typed)	Yes	505	43.6%
	No	654	56.4%
Do you keep Personally Identifiable Information (e.g. your name, bank account number etc.) on your phone?	Yes	447	38.6%
	No	654	61.4%
Do you use your phone to access the internet i.e. Facebook, Twitter, Yahoo mail, google etc.?	Yes	986	85.1%
	No	173	14.9%
Does your phone have an anti-virus program?	Yes	500	43.1%
	No	420	36.2%
	I don't know	233	20.1%
To what extent are you concerned that some files you download might collect some data from your phone without your knowledge?	Very small extent	59	5.1%
	Small extent	316	27.3%
	Never	260	22.4%
	Large extent	282	24.3%
	Very large extent	205	17.7%
Do you think information/data in your phone is important?	Yes	1014	87.5%
	No	145	12.5%
Do you have an idea of any "social engineering" tricks for mobile devices or what it means?	Yes	455	39.3%
	No	704	60.7%

Source: Compiled by the Researcher

The analysis of the "Identify" construct indicates a generally high level of awareness among respondents regarding certain mobile security practices. A significant majority, 84.8%, recognize the importance of not storing sensitive information like their MPESA PIN or mobile banking passwords as draft messages on their phones. Additionally, 85.1% actively use their

phones to access the internet, further underscoring the potential security risks associated with mobile usage. While 87.5% of respondents view the information on their devices as important, only 43.1% have installed antivirus software on their phones, and an additional 20.1% are uncertain about the presence of antivirus programs. This suggests that although respondents understand the value of their data, there is a discrepancy between awareness and the implementation of essential security measures, such as antivirus protection.

Conversely, the data highlights several areas of concern where awareness remains low. For instance, 60.7% of respondents are unfamiliar with "social engineering" tactics, exposing them to potential manipulation attacks. Furthermore, while 56.4% ensure that their phone's PIN/password is hidden when entering it, 43.6% leave it visible, which increases the risk of unauthorized access. Despite some respondents expressing concern about files collecting data without their knowledge (42.0% to a large or very large extent), a significant portion—approximately 32.4%—remains unconcerned. This indicates that although there is a general recognition of the importance of securing mobile devices, more targeted educational efforts are necessary to address the gaps in knowledge and encourage proactive measures in mitigating mobile security risks.

5.5.1.2. Analyse

Table 5.23 Distribution of Analyse in the Questionnaire

Analyse		Frequency	Percentage (%)
Have you shared your mobile money PIN/Password with others to perform a transaction?	Yes	451	38.9%
	No	708	61.1%
Have you shared your phone with someone to help you with a transaction?	Yes	434	37.4%
	No	725	62.6%
Have you shared your government registration ID card/passport to someone to withdraw MPESA for you?	Yes	394	34.0%
	No	765	66.0%
Have you set your phone to show password/PIN when entering it (so you can easily know what you typed?	Yes	983	84.8%
	No	176	15.2%
Do you enable location services on your phone?	Yes	746	64.4%
	No	266	23.0%

	I don't know	147	12.6%
Have you ever downloaded applications and documents from the internet intentionally or unknowingly?	Yes	662	57.1%
	No	497	42.9%
To what extent do you trust the safety of websites you normally access through your phone?	Unsafe most of the time	114	9.8%
	Sometimes unsafe	452	39.0%
	Generally safe	336	29.0%
	Safe most of the times	135	11.6%
	Safe all the time	122	10.5%

Source: Compiled by the Researcher

The analysis of the "Analyse" construct reveals key insights into user behaviour and attitudes towards mobile security in financial transactions. A significant majority (61.1%) of respondents refrained from sharing their mobile money PINs/passwords with others, reflecting general caution regarding security in this domain. However, 38.9% still admitted to sharing sensitive information, which highlights a potential vulnerability. Similarly, while 62.6% avoided sharing their phones for transactions, 37.4% had done so, suggesting that despite some awareness, a sizable portion of users remains at risk of exposing their sensitive data. Additionally, 66.0% reported that they did not share government identification for financial transactions, yet 34.0% did, which may indicate gaps in understanding the risks of identity theft or the necessity of protecting such personal information.

In terms of general security habits, 84.8% of respondents enabled their phones to show passwords when typing, possibly for ease of use, though this could pose a security risk. There was also a high rate of enabling location services (64.4%), potentially increasing exposure to location-based threats. Interestingly, over half of the respondents (57.1%) had downloaded applications from the internet, whether intentionally or unintentionally, which can also be a significant vector for cyber threats. Trust in website safety varied, with only 10.5% consistently feeling secure online, underscoring ongoing concerns about online security. These findings emphasize the need for increased user awareness and stricter security practices in the mobile financial environment. The risks of sharing sensitive data, using potentially insecure services,

and downloading unverified applications are critical areas for intervention in improving mobile financial security.

5.5.1.3. Train

Table 5.24 Distribution of Train in the Questionnaire

Train		Frequency	Percentage (%)
Have you ever attended an awareness session on mobile money security?	Yes	358	30.9%
	No	801	69.1%
If YES in 25 above, did you like the awareness session (i.e. was the awareness helpful to you)?	Did not answer	177	49.4%
	Yes	111	31.1%
	No	70	19.4%

Source: Compiled by the Researcher

The analysis of the "Train" construct reveals that only 30.9% of respondents have attended mobile money security awareness sessions, indicating a significant portion of the population (69.1%) has yet to be reached by such initiatives. Among those who attended, nearly half (49.4%) did not provide feedback on whether they found the sessions helpful, which could signal disengagement or inadequate mechanisms for capturing participants' input. Of the respondents who did offer feedback, 31.1% found the sessions helpful, while 19.4% expressed dissatisfaction, citing issues such as content appropriateness, delivery methods, or lack of interest.

The These findings highlight two critical areas for improvement. First, increasing outreach is essential to engage the 69.1% of respondents who have not attended any sessions. Second, the high non-response rate and dissatisfaction among participants suggest a need for better engagement strategies and content design in future awareness efforts. Enhancing the relevance, delivery, and feedback collection in mobile money security awareness initiatives could significantly improve their effectiveness and contribute to a more informed and secure user base.

5.5.1.4. Plan

Table 5.25 Distribution of Plan in the Questionnaire

Plan		Frequency	Percentage (%)
If NO in 26 above, what didn't you like in the awareness session? Tick all that apply	Did not answer	517	64.5%
	Content was not appropriate	47	5.8%
	Mode of training was not appropriate	29	3.6%
	It was not interesting	28	3.5%
	All of the above	180	22.5%
Which is of the following is your most preferred awareness delivery method? Tick your best three.			
POSTERS	No	820	70.8%
	Yes	338	29.2%
PERIODIC SMS BLASTS	No	830	71.7%
	Yes	328	28.3%
TV ADVERTS	No	466	40.2%
	Yes	692	59.8%
	Least priority	140	12.1%
	High priority	644	55.6%

Source: Compiled by the Researcher

The analysis of the "Plan" construct highlights that TV adverts are the most favoured method for delivering awareness sessions, with 59.8% of respondents preferring this medium. This suggests that audio-visual content, especially via television, is considered highly effective for reaching a broad audience and engaging participants in security-related awareness efforts. Additionally, 55.6% of respondents prioritized TV adverts as their top choice, further reinforcing the effectiveness of this medium. Periodic SMS blasts, while less preferred (28.3%), still hold value for delivering direct and timely messages, indicating that targeted communication can play a complementary role

In contrast, posters were the least favoured delivery method, with only 29.2% of respondents selecting them, suggesting that static, visual-only formats may not engage participants as

effectively as more dynamic media. Furthermore, dissatisfaction with previous awareness sessions was noted, with 22.5% of respondents indicating that all aspects—content, mode, and engagement—were lacking. This finding points to the need for improvements in session design and delivery to better meet participants' expectations and enhance overall engagement in security awareness initiatives.

5.5.1.5. Distribution of Measure and Reinforce

Table 5.26 Measure and Reinforce in the Questionnaire

Measure and Reinforce		Frequency	Percentage (%)
Are you aware of any security risks associated with using mobile devices?	Yes	872	75.2%
	No	287	24.8%
Are you aware you can disable location settings on your phone?	Yes	876	75.6%
	No	283	24.4%
Do you think mobile money security awareness is a challenge that needs to be addressed?	Yes	1068	92.2%
	No	90	7.8%
Do you think there is a need to have a mobile security education training and awareness in Kenya?	Yes	988	85.2%
	No	171	14.8%

Source: Compiled by the Researcher

The data emphasizes the widespread awareness of mobile security risks and the need for enhanced education and training among users. A significant majority of respondents, 75.2%, acknowledged their awareness of security risks associated with using mobile devices. Similarly, 75.6% reported being aware of the ability to disable location settings on their phones, suggesting a moderate understanding of security features available on mobile devices. These findings imply that a substantial portion of users possess foundational knowledge of mobile security risks and preventive measures, though there remains a notable proportion (24.8% and 24.4%, respectively) who are unaware, highlighting a gap in comprehensive awareness.

Moreover, the data indicates a strong consensus regarding the need for further action in promoting mobile money security. A striking 92.2% of respondents identified mobile money security awareness as a challenge that requires urgent attention. Additionally, 85.2% supported the implementation of mobile security education, training, and awareness programs in Kenya. These results suggest an overwhelming demand for formalized educational initiatives aimed at

mitigating security vulnerabilities in mobile financial transactions. Addressing this demand through targeted training programs could significantly enhance users' abilities to safeguard their personal and financial information, thereby reducing the risk of cyber threats and fraud.

5.5.2. Linking Survey findings to AGAM Design

To strengthen the development rationale of the Adaptive Governance Awareness Model (AGAM), Table 5.27 presents a systematic mapping of key survey findings to corresponding AGAM components. This alignment demonstrates that the model's design is empirically informed, directly addressing the specific behavioural, contextual, and awareness-related gaps identified among mobile financial services (MFS) users. For example, the 'Protect' component was included in response to widespread unsafe practices such as phone and PIN sharing, particularly among rural users. Similarly, the 'Train' and 'Plan' components were guided by findings showing that 69.1% of respondents had never attended an awareness session, and a significant portion of those who did found them ineffective. By explicitly linking model elements to observed challenges, this matrix validates the structure and relevance of AGAM, reinforcing its role as a practical and evidence-based framework for enhancing cybersecurity awareness and behaviour in the MFS context.

Table 5.27 : Mapping survey Findings to AGAM Components and Justification

Survey Finding	AGAM Component	Justification for Inclusion
Low phone protection knowledge in rural areas (only 9.6% know how to secure phone)	Protect	Highlights the need for security training on device-level practices such as passwords, screen locks, and secure access—core to the Protect function.
High rate of phone sharing (37.4%) and PIN sharing (38.9%)	Analyse	Indicates behavioural risk. "Analyse" helps in identifying and understanding risky behaviours, thus informing tailored interventions.
Majority unfamiliar with social engineering (60.7%)	Identify	Reflects low threat awareness. The Identify function promotes recognition of threats and sensitive data, justifying its inclusion for raising baseline awareness.
69.1% have never attended any awareness training	Train	A lack of formal awareness exposure necessitates structured learning initiatives to bridge this gap, which is the core focus of the Train component.
92.2% agree mobile money security awareness is a critical challenge	Govern	The broad concern supports the need for structured governance and national strategy to coordinate efforts across stakeholders.
Only 43.1% have antivirus; 20.1% unsure	Protect	Weak implementation of protective tools justifies deeper focus on security configurations and maintenance education.

Over half (57.1%) downloaded apps knowingly/unknowingly; many uncertain of website safety	Analyse / Detect	Indicates need to evaluate digital hygiene practices and implement real-time threat detection awareness strategies.
Low reporting to police/service provider in rural areas (10.1%, 11.5%)	Respond	Emphasizes the importance of building incident response capacity and clarifying reporting procedures.
Many kept quiet about financial loss—especially urban residents (31.0%–42.2%)	Respond / Recover	Shows behavioural gaps in post-incident action; justifies building user confidence in engaging support and recovering from incidents.
Longer phone ownership correlated with more secure behaviour (↓ sharing, ↑ confidence)	Reinforce	Demonstrates that experience improves security behaviour—reinforcement helps instill good habits early, rather than relying on years of exposure.
Only 30.9% attended awareness sessions; 19.4% found them unhelpful	Plan / Train	Highlights mismatch in content and delivery; the Plan function ensures content relevance, while Train refines learning strategies.
Users preferred TV ads and SMS over posters for awareness delivery	Plan	Informs the selection of effective communication channels for awareness campaigns—vital for the planning component of AGAM.
85.2% believe in need for security training in Kenya	Govern / Train	Justifies institutional and policy-based responses that scale secure behaviour training across the population.
Weak correlation between age/education and security; stronger correlation with years of phone use	Reinforce	Suggests a behavioural learning curve—supporting the inclusion of continuous reinforcement mechanisms to speed up security maturity.

Source: Compiled by author

5.5.3. Descriptive Statistics

The descriptive statistics were examined to evaluate the data and the constructs. This section presents the descriptive statistics.

5.5.3.1. Mean and Standard Deviation of Survey Items

Table 5.28 Mean and Standard Deviation of Survey Items

	Construct	Mean	Standard Deviation
Protect	P08	1.16	0.368
	P09	1.11	0.315
	P10	1.11	0.313
	P11	1.30	0.632
	P12	1.17	0.373
	P13	1.63	0.484
	P14	1.66	0.474

	P38	1.20	0.397
Detect	**D21**	**2.78**	**1.304**
	D22	1.49	0.500
	D43	3.65	1.189
	D44	1.33	0.471
	D45	1.27	0.443
Respond	**R24**	**1.39**	**1.005**
Recover	**Rc15**	**1.63**	**0.483**
	Rc16	1.66	0.472
	Rc17	3.61	1.310
Identify	**I18**	**1.15**	**0.362**
	I19	1.57	0.496
	I29	1.61	0.487
	I30	1.13	0.339
	I34	1.76	0.767
	I35	3.24	1.189
	I39	1.12	0.327
	I42	1.61	0.489
Analyse	**A14**	**1.62**	**0.486**
	A15	1.63	0.483
	A16	1.66	0.472
	A19	1.57	0.496
	A23	2.10	2.115
	A31	1.47	0.712
	A32	1.41	0.493
	A33	2.78	1.103
Govern	**G41**	**1.32**	**0.466**
	G47	1.07	0.256
	G48	1.52	0.500

Reinforce	**MR36**	**1.24**	**0.428**
	MR37	1.23	0.420
	MR47	1.07	0.256
	MR49	1.14	0.349
Plan	**PL27**	**1.18**	**1.700**
	PL28.a	0.29	0.454
	PL28.b	0.28	0.447
	PL28.c	0.22	0.411
	PL28.d	0.61	0.488
	PL28.e	0.34	0.473
	PL28.f	0.18	0.384
	PL28.g	0.12	0.325
	PL28.h	0.11	0.318
	PL28.i	0.07	0.252
	PL28.j	0.14	0.349
	PL28.k	0.07	0.256
	PL28.l	0.13	0.338
	PL28.m	0.08	0.275
Train	T25	1.69	0.462
	T26	0.71	0.775
	T50.a	1.16	0.884
	T50.b	1.22	0.913
	T50.c	1.29	0.867
	T50.d	1.21	0.923
	T50.e	1.30	0.849
	T50.f	1.24	0.905
	T50.g	1.39	0.854

Key: G = Govern, P = Protect, D = Detect, R = Respond, Rc = Recover, I = Identify, A = Analyse, PL = Plan, T = Train, MR = Reinforce

Source: Compiled by the Researcher

The analysis of the data reveals key insights into the effectiveness of various constructs in the security awareness model. The "Protect" construct demonstrates relatively low means across most survey items, with values ranging from 1.11 to 1.66, indicating a consistent perception of moderate proficiency in protection-related activities. The standard deviations, particularly for items P11 (0.632) and P13 (0.484), suggest some variability in responses, indicating that while many respondents possess moderate protection skills, there are pockets of uncertainty or lower confidence. Conversely, the "Detect" construct shows a wide range of mean values, with item D43 achieving a notably high mean (3.65) and relatively low variability (SD = 1.189). This reflects a strong consensus in the respondents' ability to detect cybersecurity threats, suggesting a well-developed capacity in this area.

Further analysis of the "Analyse" construct highlights a moderate level of analytical skills among respondents, with most items, such as A33 (Mean = 2.78, SD = 1.103), showing varying perceptions of the ability to analyse incidents effectively. The "Recover" construct, with item Rc17 (Mean = 3.61, SD = 1.310), indicates strong self-reported recovery abilities in the face of cybersecurity incidents, albeit with greater variability, suggesting differences in experience or confidence across respondents. In contrast, the "Plan" construct presents lower mean values, particularly for items PL28.b through PL28.m, with means ranging from 0.07 to 0.61, indicating a potential gap in planning capabilities.

The findings suggest that while respondents generally perceive themselves as having strong abilities in areas such as detection (D43) and recovery (Rc17), there are notable weaknesses in areas like planning (PL28 series) and governance (G47). The variability across items reflects differing levels of confidence in these abilities, pointing to the need for targeted improvements in specific areas of security awareness. In particular, enhancing governance, planning, and reinforcement may bolster the overall effectiveness of cybersecurity awareness programs. Additionally, the relatively strong detection and analytical capabilities should be leveraged to further strengthen the cybersecurity posture of the surveyed population.

5.5.3.2. Reliability Coefficients

Reliability coefficient measures the consistency or dependability of a set of measurements or test scores. It indicates the extent to which the measurements or scores are free from measurement error and provide consistent results over time or across different conditions.

Table 5.29 Reliability Coefficients

Construct	Cronbach's α	Composite Reliability
Protect	0.819	0.842
Detect	0.747	0.814
Respond	0.674	0.721
Recover	0.680	0.732
Identify	0.667	0.822
Analyse	0.771	0.837
Govern	0.701	0.804
Plan	0.734	0.870
Train	0.810	0.921
Reinforce	0.784	0.912

Source: Compiled by the Researcher

The survey items for each construct exhibit varying levels of internal consistency reliability, as indicated by Cronbach's α and Composite Reliability (CR) values. For instance, the constructs show Cronbach's α ranging from 0.667 (Identify) to 0.819 (Protect), suggesting moderate to high levels of internal consistency. Composite Reliability values range from 0.721 (Respond) to 0.921 (Train), indicating that the constructs generally have good to excellent reliability in measuring their respective dimensions.

Two key findings can be highlighted from the data:

- **Train Reliability**: The construct 'Train' demonstrates the highest reliability with a Cronbach's α of 0.810 and a Composite Reliability of 0.921. This indicates that the survey items related to training practices are highly consistent in measuring the intended aspects within this construct. High reliability in training is crucial as it ensures that the survey items reliably capture respondents' perceptions or experiences related to training effectiveness and adequacy.
- **Respond and Recover Reliability**: Conversely, the constructs 'Respond' and "Recover" show relatively lower reliability coefficients with Cronbach's α values of 0.674 and 0.680, respectively, and Composite Reliability values of 0.721 and 0.732. These lower values suggest that while the survey items within these constructs still

demonstrate acceptable levels of internal consistency, there may be some variability in how reliably they measure the aspects of response and recovery capabilities. This could potentially influence the precision and generalizability of findings related to these constructs in the study.

5.5.3.3. Convergent Validity

Convergent validity is a concept used in research methodology, particularly in the context of measurement validation. It refers to the extent to which different methods of measuring the same construct or concept produce similar results. In other words, it assesses whether multiple measures that are supposed to be measuring the same thing are actually converging or yielding consistent results.

Table 5.30 Convergent Validity

Construct	AVE Value
Protect	0.658
Detect	0.643
Respond	0.532
Recover	0.510
Identify	0.660
Analyse	0.645
Govern	0.554
Plan	0.713
Train	0.621
Reinforce	0.707

Source: Compiled by the Researcher

The analysis of the provided Average Variance Extracted (AVE) values for the survey items is conducted to assess the convergent validity of each construct. Convergent validity is confirmed when the AVE value for a construct is at least 0.50, indicating that more than 50% of the variance of the construct is due to its indicators.

The AVE values indicate that all constructs have acceptable levels of convergent validity. Specifically, the constructs ‘Plan’ (0.713) and ‘Reinforce’ (0.707) exhibit the highest AVE values, demonstrating strong convergent validity. These high AVE values suggest that the

items measuring these constructs are highly correlated and effectively capture the underlying construct. Conversely, the constructs 'Respond' (0.532) and 'Recover' (0.510) have the lowest AVE values among the constructs, but they still meet the minimum threshold for convergent validity, indicating that the items are adequately representative of these constructs.

5.5.3.4. Discriminant Validity

Discriminant validity refers to the extent to which a construct or test measures what it is supposed to measure, distinctly from other constructs or tests. It assesses whether concepts or measurements that are supposed to be unrelated are, in fact, unrelated. This type of validity is crucial for establishing the uniqueness of a construct and ensuring that it is not merely a reflection of other variables.

Table 5.31 Discriminant Validity

	P	D	R	Rc	I	A	G	PL	T	MR
P	**0.658**									
D	-0.274	**0.643**								
R	0.255	0.155	**0.532**							
Rc	0.123	0.091	0.104	**0.510**						
I	**0.331**	**-0.371**	0.324	0.280	**0.660**					
A	-0.278	**0.402**	0.236	0.208	**0.375**	**0.645**				
G	0.061	0.260	**0.491**	0.291	0.175	0.160	**0.554**			
PL	**0.438**	-0.085	0.143	**0.351**	**0.542**	0.111	0.102	**0.713**		
T	-0.139	**0.513**	0.129	0.152	0.224	0.226	**0.391**	**0.305**	**0.621**	
MR	**0.338**	-0.185	**0.328**	**0.228**	0.381	0.141	0.216	0.155	0.252	**0.707**

Key: G = Govern, P = Protect, D = Detect, R = Respond, Rc = Recover, I = Identify, A = Analyse, PL = Plan, T = Train, MR = Reinforce

Source: Compiled by the Researcher

The discriminant validity results demonstrate that each construct within the model is sufficiently distinct from others, as indicated by the square root of the average variance extracted (AVE) values on the diagonal. These values, ranging from 0.510 to 0.713, exceed most of the inter-construct correlation values. For example, the construct 'Protect' (0.658)

shows a higher value compared to its correlations with other constructs, such as its correlation with 'Govern' (0.061) and 'Respond' (0.255), confirming its discriminant validity. This suggests that the constructs are successfully capturing unique concepts, which is essential for the model's reliability.

In conclusion, the discriminant validity results affirm the robustness of the constructs in distinguishing between various aspects of user awareness for mobile financial services. This ensures that the constructs can be reliably used in further analysis without significant risk of measuring overlapping concepts, thereby enhancing the credibility of the model.

5.5.3.5. Outer Variance Inflation Factor

Next, variance inflation factor (VIF) values identified potential multicollinearity issues within the model. Table 5.37 presents the VIF values for the construct items. VIF values greater or equal to 1 and less than 5 indicate no presence of multicollinearity. The results reported in Table 5.37 show no evidence of multicollinearity for any construct entered in the model.

Table 5.32 Variance Inflation Factor

	Construct	VIF
Protect	**P08**	**1.182**
	P09	1.244
	P10	1.464
	P11	1.700
	P12	1.197
	P13	1.452
	P14	1.244
	P38	1.316
Respond	**R24**	**1.309**
Recover	**Rc15**	**1.498**
	Rc16	1.297
	Rc17	1.325
Govern	**G41**	**1.315**
	G47	1.620

	G48	1.413
Detect	**D21**	**1.046**
	D22	1.810
	D43	1.287
	D44	1.290
	D45	1.188
Identify	**I18**	**1.159**
	I19	1.085
	I29	1.194
	I30	1.276
	I34	1.440
	I35	1.090
	I39	1.355
	I42	1.064
Analyse	A14	1.178
	A15	1.161
	A16	1.236
	A19	1.463
	A23	1.661
	A31	1.193
	A32	1.429
	A33	1.114
Measure and Reinforce	**MR36**	**1.507**
	MR37	1.684
	MR47	1.509
	MR49	1.320
Train	**T25**	**1.683**
	T26	1.437

	T50.a	1.617
	T50.b	1.824
	T50.c	1.343
	T50.d	1.488
	T50.e	1.293
	T50.f	1.114
	T50.g	1.245
Plan	**P27**	**1.623**
	P28.a	1.417
	P28.b	1.060
	P28.c	1.819
	P28.d	1.311
	P28.e	1.319
	P28.f	1.274
	P28.g	1.080
	P28.h	1.220
	P28.i	1.211
	P28.j	1.219
	P28.k	1.347
	P28.l	1.482
	P28.m	1.734

Key: G = Govern, P = Protect, D = Detect, R = Respond, Rc = Recover, I = Identify, A = Analyse, PL = Plan, T = Train, MR = Reinforce

Source: Compiled by the Researcher

5.5.3.6. Confirmatory Factor Analysis

After examining the VIF values, a confirmatory factor analysis (CFA) was conducted to assess the validity and reliability of the proposed model's structure. The CFA was carried out to validate the theoretical constructs and to assess the measurement model fit. To achieve these, a number of tests were conducted as highlighted in the subsequent sections.

a) CMIN

Model	NPAR	CMIN	df	P	CMIN/DF
Default Model	28	1232.309	27	0.000	2.641
Saturated Model	55	0.000	0		
Independence Model	10	2489.682	45	0.000	55.326

Source: Compiled by the Researcher

b) RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default Model	0.028	0.952	0.898	0.818
Saturated Model	0.000	1.000		
Independence Model	0.044	0.677	0.605	0.554

Source: Compiled by the Researcher

Chi-Square

Chi-square = 32.309

Degrees of freedom = 27

Probability level = .000

c) Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default Model	0.905	0.875	0.911	0.978	0.907
Saturated Model	1.000		1.000		1.000
Independence Model	0.000	0.000	0.000	0.000	0.000

Source: Compiled by the Researcher

d) **RMSEA**

Model	RMSEA	LO 90	HI 90	PCLOSE
Default Model	0.047	0.187	0.206	0.201
Independence Model	0.217	0.209	0.224	0.000

Source: Compiled by the Researcher

The Confirmatory Factor Analysis (CFA) results indicate an acceptable model fit for the awareness model. The chi-square test, although significant ($\chi^2 = 32.309$, df = 27, $p < .001$), is expected given the sample size. The CMIN/DF value of 2.641 falls within the acceptable range of 2–5, confirming an adequate fit. Furthermore, the Goodness of Fit Index (GFI = .952) and Adjusted GFI (AGFI = .898) both reflect a strong fit, approaching the threshold of .90. Comparative fit indices are favourable, with the Normed Fit Index (NFI = .905), Comparative Fit Index (CFI = .907), and Incremental Fit Index (IFI = .911) all exceeding the .90 benchmark. The high Tucker-Lewis Index (TLI = .978) further supports the model's robustness.

The Root Mean Square Residual (RMR = .028) is well below the recommended .05, indicating good fit. The Root Mean Square Error of Approximation (RMSEA = .047) suggests a well-fitting model, being under the .05 threshold, while the PCLOSE value of .201 indicates acceptable parsimony. Additionally, the Parsimony Goodness-of-Fit Index (PGFI = .818) demonstrates that the model balances goodness of fit with complexity. Overall, the results suggest a model that is both well-fitting and parsimonious.

5.6. VALIDATION OF THE PROPOSED MODEL

At the start of this study, the researcher developed a theoretical model that was the lens through which cybersecurity posture was to be investigated. A number of tests were carried out to validate the proposed framework. One of the tests carried out was Structural Equation Model (SEM). This was used because it is a confirmatory technique that allows for the testing of hypothesized relationships between latent variables and the cybersecurity and measured variables (Protect, detect, respond, and recover). This technique is also appropriate because it allows for the use of multiple measured variables (constructs from the theoretical frameworks) to better understand the cybersecurity posture of the MFS users.

Using the question mobile money security awareness as the dependent variable, the results of the model were as follows:

5.6.1. Model summary

Table 5.33 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.709[a]	.503	.499	.251	.503	116.354	10	1148	.000

a. Predictors: (Constant), Train, Govern, Respond, Recover, Detect, Protect, Plan, Identify, Analyse, and Reinforce.

b. Dependent Variable: Do you think there is a need to have a mobile security education training and awareness in Kenya?

Source: Compiled by the Researcher

The model summary demonstrates the relationship between various predictors (Train, Govern, Respond, Recover, Detect, Protect, Plan, Identify, Analyse, and Reinforce) and the dependent variable: the perceived necessity for mobile security education and awareness in Kenya. The R value of 0.709 indicates a strong positive correlation between the predictors and the dependent variable, suggesting that these constructs collectively have a substantial influence on the perception of the need for mobile money security awareness. This correlation value implies that as the effectiveness of these predictors increases, so does the recognition of the necessity for such awareness initiatives.

The R Square value of 0.503 indicates that 50.3% of the variability in the perception of the need for mobile security education is explained by the model. This marks a significant improvement compared to the previous interpretation, indicating that the model has strong explanatory power. The Adjusted R Square value of 0.499, closely aligned with the R Square value, further validates that the model does not suffer from overfitting, and the inclusion of multiple predictors remains appropriate for explaining the dependent variable.

The significance of the model is further reinforced by the F-statistic ($F = 116.354$) and the associated p-value ($p = 0.000$), which confirm that the predictors contribute meaningfully to the regression model. Additionally, the Standard Error of the Estimate (0.251) reflects a good fit of the data, with the observed values falling relatively close to the predicted regression line. These statistics collectively indicate that the model is both statistically significant and robust in explaining the factors influencing the necessity for mobile security education and awareness in Kenya.

5.6.2. Analysis of Variance (ANOVA)

Table 5.34 Analysis of Variance (ANOVA) Results

	Model	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	73.375	10	7.338	116.354	.000[b]
	Residual	72.395	1148	.063		
	Total	145.770	1158			

a. Dependent Variable: Do you think there is a need to have a mobile security education training and awareness in Kenya?

b. Predictors: (Constant), Train, Govern, Respond, Recover, Detect, Protect, Plan, Identify, Analyse, and Reinforce.

Source: Compiled by the Researcher

ANOVA Results Analysis

The analysis of variance (ANOVA) results indicate that the regression model significantly predicts the perceived need for mobile security education training and awareness in Kenya. The regression sum of squares (73.375) reflects the amount of variation in the dependent variable explained by the predictors (Train, Govern, Respond, Recover, Detect, Protect, Plan, Identify, Analyse, and Reinforce), while the residual sum of squares (72.395) represents the unexplained variation. The high F-value (116.354) and the significance level ($p = 0.000$) confirm that the model is statistically significant, rejecting the null hypothesis and indicating that the predictors collectively contribute to the model's explanatory power.

Thus, it can be concluded that the independent variables have a significant impact on the perceived need for mobile security education training and awareness. The model provides strong evidence that factors such as training, governance, response, and protection are crucial in shaping user awareness, emphasizing the relevance of these constructs in developing effective security awareness programs for mobile financial services in Kenya.

5.6.3. Path Analysis

After ensuring acceptable fit through model construct evaluation, a PLS-SEM path analysis was performed. The path analysis for the PLS-SEM model is depicted in Figure 5.5.

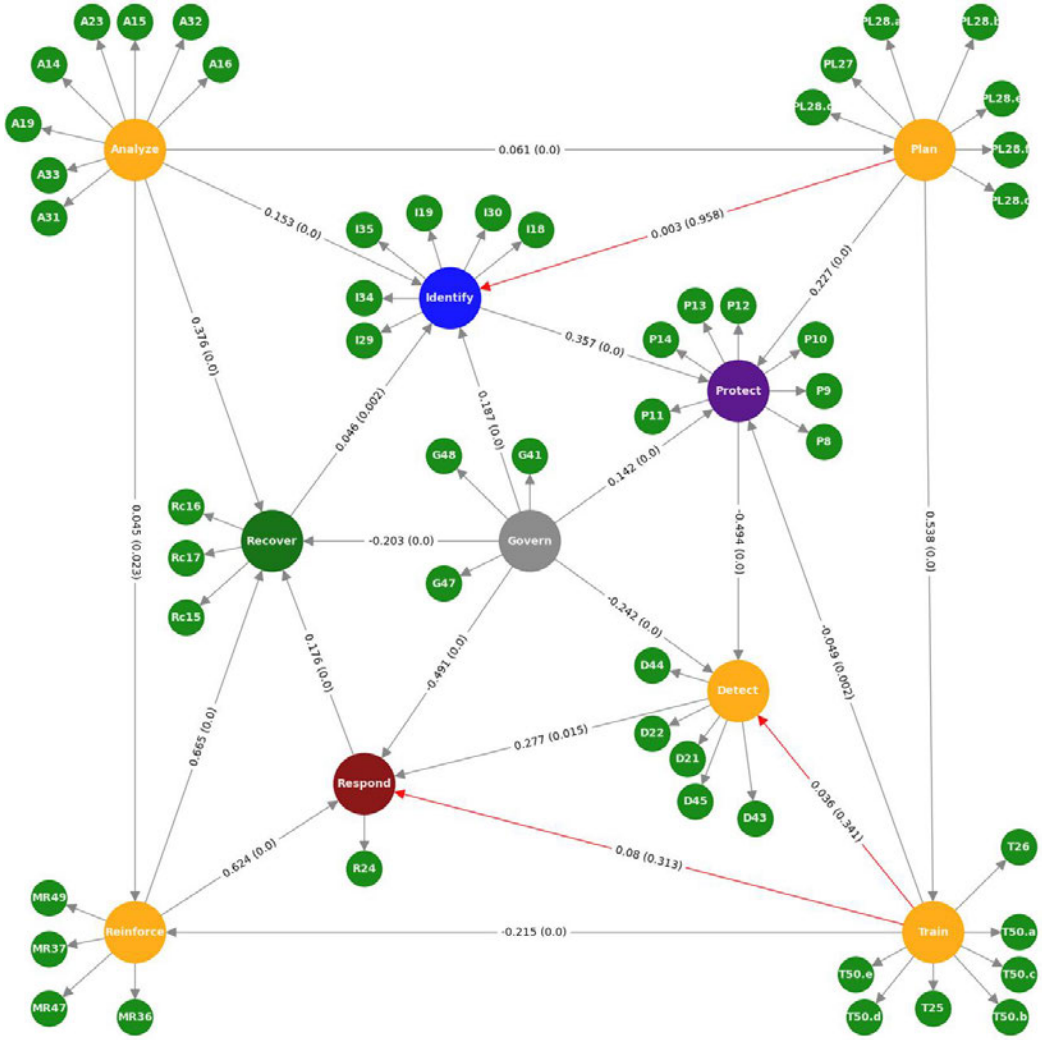


Figure 5.5 Path Analysis Model

Source: Compiled by the Researcher

The strength and significance of each path coefficient are displayed, with significance values indicated in parentheses. Significant relationships between model constructs are denoted by green arrows ($p < 0.05$), while red arrows indicate nonsignificant relationships ($p > 0.05$).

Table 5.42 presents the hypothesis testing results from the path analysis in tabular format. The path coefficients illustrate the strength and direction of variable relationships tested for the study's hypotheses, while p-values indicate the statistical significance of these relationships. P-values below 0.05 signify significant relationships.

Table 5.35 The Results of the Hypothesis Testing

Paths	Estimate	S.E.	C.R.	P	Hypothesis Results
I <--- G	0.187	0.022	8.397	***	Accept
P <--- G	0.142	0.022	6.329	***	Accept
D <--- G	-0.242	0.054	-4.515	***	Accept
R <--- G	-0.491	0.105	-4.683	***	Accept
Rc <--- G	-0.203	0.039	-5.198	***	Accept
R <--- D	0.277	0.029	3.535	0.015	Accept
Rc <--- R	0.176	0.011	16.248	***	Accept
I <--- Rc	0.046	0.015	3.050	0.002	Accept
PL <--- A	0.061	0.010	6.170	***	Accept
T <--- PL	0.538	0.092	5.837	***	Accept
MR <--- T	-0.215	0.018	-11.691	***	Accept
P <--- T	-0.049	0.016	-3.027	0.002	Accept
P <--- PL	0.227	0.052	4.398	***	Accept
I <--- PL	0.003	0.051	0.053	0.958	Reject
P <--- I	0.357	0.028	12.593	***	Accept
I <--- A	0.153	0.019	8.268	***	Accept
Rc <--- A	0.376	0.031	12.229	***	Accept
MR <--- A	0.045	0.020	2.266	0.023	Accept
R <--- MR	0.624	0.114	5.487	***	Accept
D <--- T	0.036	0.038	0.953	0.341	Reject
D <--- P	-0.494	0.065	-7.615	***	Accept
R <--- MR	0.665	0.120	5.537	***	Accept
R <--- T	0.080	0.080	1.009	0.313	Reject

Key: G = Govern, P = Protect, D = Detect, R = Respond, Rc = Recover, I = Identify, A = Analyse, PL = Plan, T = Train, MR = Reinforce.

Source: Compiled by the Researcher

The table presents results from the path analysis conducted to test various hypotheses regarding the relationships between constructs. Each path represents a hypothesized relationship between variables. Each path was analysed to determine the significance of the estimated coefficients, as indicated by the critical ratio (C.R.) and p-values. A hypothesis is considered supported if the P value is less than 0.05, indicating that the relationship is statistically significant.

The path from **Govern (G) to Identify (I)** demonstrated a positive and significant estimate of 0.187 with a critical ratio of 8.397 ($p < 0.001$). This suggests that the govern construct has a significant positive influence on the identify construct, supporting the acceptance of the hypothesis. Similarly, the path from **Govern (G) to Protect (P)** was also positive and significant, with an estimate of 0.142, a critical ratio of 6.329, and a p-value less than 0.001, leading to the acceptance of this hypothesis.

On the contrary, the paths from **Govern (G) to Detect (D)**, **Respond (R)**, and **Recover (Rc)** were negative yet significant, with respective estimates of -0.242, -0.491, and -0.203, indicating that as the govern construct increases, these three variables decrease. Despite the negative coefficients, the p-values (all < 0.001) confirm the rejection of the null hypotheses and the acceptance of these relationships.

The path from **Detect (D) to Respond (R)** showed a positive relationship with an estimate of 0.277 and a critical ratio of 3.535 ($p = 0.015$), confirming a significant positive relationship between these two constructs, hence supporting the hypothesis. Moreover, the path from **Respond (R) to Recover (Rc)** was found to be highly significant with an estimate of 0.176 and a critical ratio of 16.248 ($p < 0.001$), which leads to the acceptance of this hypothesis as well.

A noteworthy finding is that the path from **Plan (PL) to Identify (I)** was not significant (estimate = 0.003, C.R. = 0.053, $p = 0.958$), leading to the rejection of this hypothesis. Additionally, the path from **Train (T) to Detect (D)** was also non-significant (estimate = 0.036, $p = 0.341$), and thus, the hypothesis was rejected. Similarly, the path from **Train (T) to Respond (R)** was not significant ($p = 0.313$), leading to its rejection.

Conversely, the path from **Analyse (A) to Identify (I)** was significant, with an estimate of 0.153 and a critical ratio of 8.268 ($p < 0.001$), leading to the acceptance of the hypothesis. Furthermore, the relationship between **Analyse (A) and Recover (Rc)** was significant, with an estimate of 0.376 (C.R. = 12.229, $p < 0.001$). The path from **Analyse (A) to Reinforce (MR)**

also displayed significance (estimate = 0.045, p = 0.023), supporting the hypothesis that Analyse influences Reinforcement strategies.

Finally, paths such as **Train (T) to Plan (PL)**, **Reinforce (MR) to Respond (R)**, and **Respond (R) to Recover (Rc)** were all highly significant with p-values less than 0.001, confirming the acceptance of these hypotheses. The strong path from **Plan (PL) to Protect (P)** (estimate = 0.227, $p < 0.001$) further supports the significant relationship between planning and protection strategies.

The data analysis revealed that the majority of the hypothesized paths were supported, demonstrating statistically significant relationships between the variables. Specifically, 20 paths were found to be significant, while 3 paths did not show statistical significance. This comprehensive analysis provided robust evidence supporting the majority of the proposed hypotheses, contributing to the understanding of the relationships among the studied variables. The findings strongly supported the relationships between key constructs in the model, with "govern," "analyse," and "train" demonstrating substantial influence across multiple variables in the adaptive governance model.

5.6.4. Final Model

The final model that shows the relationship among the constructs borrowed from NIST cybersecurity and MediaPro adaptive Awareness frameworks that help to improve cybersecurity behaviour of users of mobile financial services. Figure 5.6 depicts the final representation of the Adaptive Governance Awareness Model (AGAM).

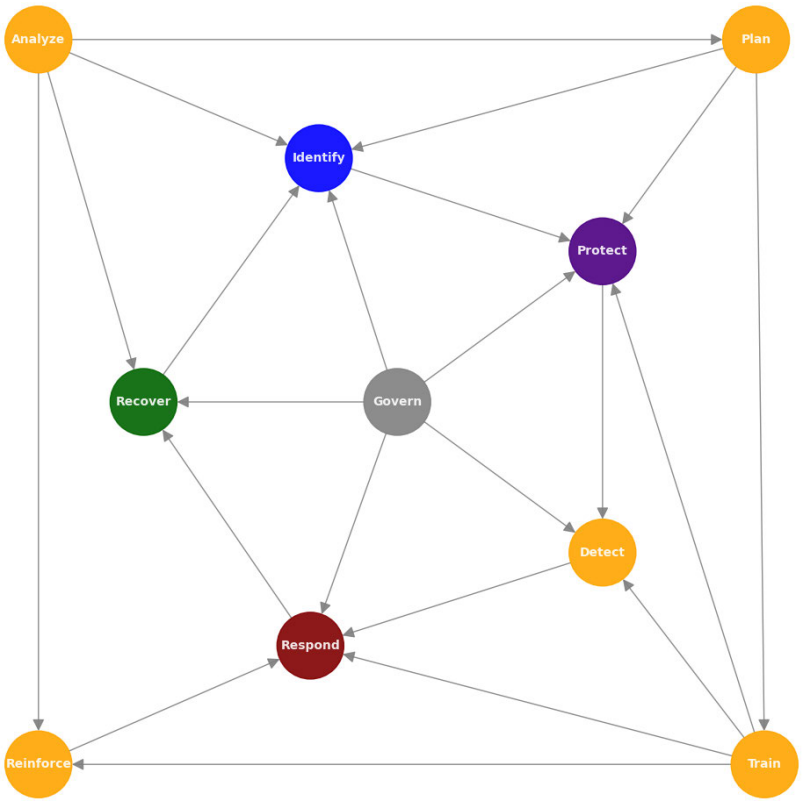


Figure 5.6: Final Representation of the Adaptive Governance Awareness Model (AGAM)

Source: Compiled by the Researcher

A two-dimensional representation of AGAM showing the interaction of the constructs is depicted in Figure 5.7.

Figure 5.7 A Two-Dimensional Representation of AGAM

Source: Compiled by the Researcher

Key Elements of AGAM:

Central Core: Govern

- **Govern** is at the centre, highlighting its role in overseeing and integrating all processes.

Inner Ring: NIST Functions

- Surrounding **Govern** are the NIST functions: **Identify, Protect, Detect, Respond, Recover**, arranged in a circular manner.

Outer Ring: MediaPro Functions

- Encapsulating the NIST functions, the MediaPro functions: Analyse, Plan, Train and Reinforce.

Interactions and Dependencies:

The arrows indicate the interaction and support between the MediaPro and NIST functions

1. **Govern** (Central)
    - **Identify:** Governance involves identifying policies, roles, and responsibilities.
    - **Protect:** Governance ensures protective measures are in place.
    - **Detect:** Governance mandates the need for detection mechanisms.
    - **Respond:** Governance dictates response protocols.
    - **Recover:** Governance oversees recovery strategies.
2. **Identify ⇨ Protect:** Identifying assets, threats, and vulnerabilities informs the protection mechanisms.
3. **Protect ⇨ Detect:** Protection mechanisms need to be monitored, thus leading to detection.
4. **Detect ⇨ Respond:** Detection of incidents triggers response actions.
5. **Respond ⇨ Recover:** Responding to incidents often includes steps that overlap with recovery processes.
6. **Recover ⇨ Identify:** Post-recovery analysis identifies gaps and informs future identification processes.

7. **Analyse ⇨ Plan:** Analysing current awareness levels informs planning.
8. **Plan ⇨ Train:** Planning leads to the development of training programs.
9. **Train ⇨ Reinforce:** Training needs to be reinforced for long-term effectiveness.
10. **Reinforce ⇨ Analyse:** Reinforcement activities provide data that feeds back into analysis.
11. **Analyse ⇨ Identify:** Analysis helps in identifying gaps in cybersecurity awareness.
12. **Plan ⇨ Protect:** Planning awareness programs aligns with protecting resources.
13. **Train ⇨ Detect:** Training improves detection capabilities.
14. **Reinforce ⇨ Respond:** Reinforcement ensures prompt and effective response.
15. **Reinforce ⇨ Recover:** Reinforcement improves recovery capabilities.
16. **Analyse ⇨ Recover:** Continuous analysis aids in improving recovery processes.

Relationship Between Outer and Middle Layers:

The outer layer of MediaPro Adaptive Awareness constructs—*Analyse, Plan, Train and Reinforce*—is designed to support and strengthen the inner NIST constructs—*Identify, Protect, Detect, Respond, Recover*. The connections between these two layers reflect the dynamic and iterative nature of cybersecurity awareness.

- **Analyse to Identify and Recover**: Analysis plays a pivotal role in both identifying risks and informing the recovery process. Continuous analysis ensures that threat identification is informed by up-to-date data and that recovery efforts are refined based on the latest security trends and threat landscapes. Through regular assessment of risks and vulnerabilities, the model ensures that identification is informed by current insights, and recovery processes are constantly evolving to address newly emerging threats.
- **Plan to Protect**: Planning establishes the groundwork for identifying threats and implementing protective measures.
- **Train to Protect and Respond**: Training is essential for equipping users with the necessary skills to protect against threats, detect potential attacks, and respond appropriately. The relationship between training and detection may be weak in isolation, but it remains vital for strengthening protective measures and ensuring that users are prepared to respond to cybersecurity incidents.

- **Reinforce to Respond and Recover**: Continuous reinforcement strengthens the ability of users to effectively respond to and recover from incidents. Reinforcing security behaviours ensures that lessons learned are consistently applied, improving resilience over time. Reinforcement strengthens users' ability to respond to security threats and recover from incidents by embedding best practices into their routine behaviour.

Importance of Relationships within the Model:

- **Govern at the Centre**: At the heart of the model, *Govern* serves as the guiding force, ensuring oversight and consistent application of policies. It drives the processes in the surrounding NIST constructs, ensuring that identification, protection, detection, response, and recovery are all aligned with governance principles. As the central construct, *Govern* provides oversight and strategic direction for all other components in the model. Governance ensures that the processes of identifying, protecting, detecting, responding, and recovering are aligned with overarching policies and standards. By placing *Govern* at the centre, the model emphasizes the importance of a structured, top-down approach to cybersecurity.
- **Sequential Flow of NIST Constructs**: The cyclical nature of the inner layer—*Identify to Protect to Detect to Respond to Recover*—represents the core lifecycle of information security. This continuous loop ensures that mobile financial service users are engaged in an adaptive security process, from threat identification to recovery, and then back to the start of the loop. This flow ensures that each step feeds into the next, creating a resilient system where threats are identified early, managed effectively, and followed by swift recovery, creating a self-sustaining security awareness process.
- **Adaptive Awareness through MediaPro Constructs**: The outer layer introduces adaptability through *Analyse, Plan, Train and Reinforce*. These constructs ensure that the awareness efforts are not static but evolve based on ongoing feedback and adaptation. The interactions between the outer and inner layers enable continuous improvement, making the model responsive to new threats and vulnerabilities as they emerge. These constructs ensure that the awareness process remains dynamic, adaptive, and continually evolving. By feeding into the NIST constructs, the outer layer ensures that strategic planning, training, analysis, and reinforcement contribute to core security processes, ensuring that users of mobile financial services remain aware and responsive to evolving threats.

Justification for AGAM Model Components:

The development of the Adaptive Governance Awareness Model (AGAM) was informed by the need to improve cybersecurity awareness and behaviour within the mobile financial services (MFS) ecosystem, particularly in developing economies such as Kenya. AGAM integrates carefully selected components from two foundational frameworks: the NIST Cybersecurity Framework and the MediaPro Adaptive Awareness Framework. However, AGAM is not a direct adaptation of either model. Instead, it represents a novel synthesis informed by literature, contextual realities, and empirical evidence drawn from a comprehensive survey of 1,159 MFS users across Kenya.

A key innovation introduced in AGAM is the "Govern" construct, which is not present in either NIST or MediaPro. This component emerged from the observed disconnection between policy-level cybersecurity strategies and actual user awareness needs—a concern echoed by Bada et al. (2019), who argue that many African cybersecurity strategies lack clear implementation mechanisms or coordination. While governance is implicit in NIST through references to risk management strategy (NIST, 2018), AGAM elevates it to an explicit and overarching construct. Survey findings revealed that 69.1% of respondents had never attended any cybersecurity awareness training, and among the few who had, 22.5% rated the training content or mode as ineffective. The lack of strategic coordination and user-oriented delivery mechanisms underlines the need for a governance layer that ensures awareness programs are well-planned, budgeted, context-sensitive, and institutionally anchored (World Bank, 2020). Furthermore, the disconnect between preferred training delivery formats (59.8% of users preferred TV while only 28.3% preferred SMS) highlights a governance failure to tailor content effectively. By embedding "Govern" into AGAM, the model bridges the gap between policy and practice, enabling a systemic and coordinated approach to user education.

The "Identify" construct was adapted from NIST's core functions, which begin with asset and risk identification. However, NIST's framing is largely institutional, assuming a level of security awareness and IT infrastructure that is not present among most MFS users. Survey data revealed that 15.2% of respondents stored MPESA PINs in phone drafts, and 56.4% exposed their PINs while typing, indicating a fundamental lack of awareness about what constitutes sensitive information. Additionally, 60.7% of users had no knowledge of social engineering tactics. These findings mirror broader research showing that digital literacy significantly moderates security behaviour in digital finance (Al-Doghan & Mirzaliev, 2024).

Retaining the “Identify” function in AGAM enables users to recognize the value of their personal and financial data and to understand the threats targeting such assets.

The “Protect” function is equally relevant in the MFS context, where many users operate on low-end devices with minimal built-in security features. Survey findings showed that only 46% of respondents aged 18–25 had enabled password protection on their phones, and users with lower education levels or living in rural areas were significantly less likely to implement basic protective measures. These results align with findings that security awareness is lower in digitally excluded populations, and protective habits are limited when access to structured training is lacking (de Bruijn & Janssen, 2017). AGAM incorporates “Protect” to promote simple but effective actions such as locking devices, managing app permissions, and safeguarding credentials, tailored to users’ literacy levels and technological environments.

The “Detect” function is included in AGAM to address users’ ability to recognise when their security has been compromised. While NIST defines detection as continuous monitoring for threats (NIST, 2018), AGAM contextualises it for individuals who may not have access to technical monitoring tools. Only 31.9% of young users (18–25 years old) in the study believed they could always tell if their phones had been hacked. Detection skills correlated strongly with education, indicating the need to raise user capacity to identify phishing, SIM swaps, and unauthorized access. Recent studies show that human-centric threat recognition is vital, as over 70% of breaches involve social engineering and human error (Verizon, 2023). AGAM’s “Detect” function therefore focuses on enhancing situational awareness through examples, analogies, and threat simulations appropriate for non-technical users.

AGAM also incorporates the “Respond” function, redefined to suit end-user realities. According to the survey, approximately 20% of users who experienced mobile money fraud or data breaches chose to remain silent, particularly in rural areas where reporting mechanisms were either unavailable or poorly understood. This aligns with research by the World Bank (2020), which emphasizes that users often lack clear post-incident guidelines. AGAM’s “Respond” function equips users with actionable steps to take following a breach, including reporting to service providers, changing credentials, and alerting authorities or contacts.

The “Recover” component supports individual users in regaining control after an incident. While NIST (2018) describes recovery as ensuring operational continuity for organizations, AGAM adapts the concept to support individuals. Survey results showed that around 20% of users who had suffered mobile money fraud chose not to act—often due to unclear reporting

mechanisms or distrust in the system. Research in Kenya finds that applying interactional justice strategies during service recovery (e.g., respectful and fair treatment) significantly improves customer satisfaction and future engagement with the service (Ngahu, Kibera, & Kobonyo, 2022). Embedding recovery guidance in AGAM aligns with these principles, helping users feel supported and confident in taking remedial actions.

AGAM further extends beyond NIST by incorporating four behavioural and educational components from the MediaPro Adaptive Awareness Framework: "Analyse," "Plan," "Train," and "Reinforce." The "Analyse" function supports the need for continuous evaluation of users' knowledge and behaviours. The survey revealed critical gaps—38.9% of users had shared their PINs and 34% had shared their ID cards. These findings by Alshehri et al (2023) align with recent research showing that behavioural assessments must precede the design of cybersecurity awareness programs in order to tailor content to users' risk profiles, cognitive patterns, and digital contexts. This supports AGAM's emphasis on ongoing, personalized training and reinforcement strategies.

The "Plan" function addresses demographic disparities in awareness preferences. Only 30.9% of users had attended an awareness session, and 22.5% of those found it ineffective. Urban users preferred visual content while rural users preferred audio. The MediaPro model supports adaptive planning that matches delivery modes with audience profiles (MediaPro, 2016).

"Train" remains central to behavioural change. Recent research emphasises the value of role-based, adaptive, and continuous cybersecurity training, showing that personalised programs tailored to users' knowledge levels and digital environments significantly improve engagement and retention (Alshehri et al., 2023). AGAM adapts this to the MFS context where digital literacy varies widely. Survey findings showed uneven knowledge across age, education, and location. AGAM's "Train" function supports repeated engagement through accessible channels like community workshops, radio, and apps—approaches shown to work effectively in low-literacy environments as highlighted by Ombati et al. (2021).

Finally, "Reinforce" addresses the persistence gap between knowledge and secure behaviour. Despite some awareness, many users continued risky habits like displaying PINs or sharing devices. Empirical research shows that gamification and behavioural nudges significantly improve engagement, retention, and behaviour change in cybersecurity training, especially when programs include storytelling, leaderboards, and real-world simulations (Pramod, 2024).

In summary, AGAM's structure is both empirically grounded and contextually relevant. It differentiates itself from NIST by incorporating user-centred planning and behavioural reinforcement mechanisms, and from MediaPro by incorporating core security lifecycle functions. Moreover, it introduces the unique "Govern" layer, which aligns top-down policy and institutional strategies with grassroots user engagement. This layered and adaptive architecture ensures that AGAM not only improves awareness but fosters sustainable behavioural change among diverse MFS users in developing contexts.

5.7. IMPLEMENTATION STRATEGY FOR AGAM

This section provides guidelines in a tabular format for the activities that need to be carried in each function of the framework and the desired outcomes in order for organisations to realise the benefits of AGAM.

Table 5.36 The Implementation Strategy For AGAM

Function	Activities	Outcomes
Govern: Establish Robust Governance Policies	• Develop comprehensive cybersecurity policies for mobile financial services that align with organizational goals. • Ensure regulatory compliance by adhering to relevant laws and guidelines. • Implement effective risk management strategies to mitigate cybersecurity risks.	• A clear set of policies that guide cybersecurity practices. • Compliance with legal and regulatory requirements. • Reduced risk of cybersecurity incidents through proactive management.
Identify: Educate Users and Inventory Management	• Conduct awareness campaigns to educate users of mobile financial services about the personal information stored on their phones and potential threats. • Encourage users to maintain an inventory of their digital devices. • Train users to secure their mobile devices used for accessing financial information.	• Increased user awareness of personal information security. • Users have a clear understanding of potential threats like phishing and unauthorized access. • Users maintain a secure inventory of their devices.

Protect: Training on Security Practices	• Provide training on creating and managing strong passwords and the importance of not sharing them. Users should implement good password practices i.e. not using year of birth. • Educate users on implementing biometric and multifactor authentication. • Promote the regular updating of financial applications and mobile device operating systems. • Emphasize the importance of data encryption and using secure connections.	• Users implement strong, unique passwords and understand the importance of keeping them confidential. Users having good password practices. • Increased use of biometric and multifactor authentication. • Regularly updated applications and operating systems reduce vulnerabilities. • Enhanced data protection through encryption and secure connections.

Function	Activities	Outcomes
Detect: Recognize and Respond to Unusual Activities	• Train users to recognize unusual account activities, such as unexpected transactions or login attempts. • Encourage the setup of notifications and alerts for suspicious activities.	• Users can identify and report unusual activities promptly. • Early detection of suspicious activities through notifications and alerts.
Respond: Reporting and Immediate Action	• Educate users on how to report suspicious activities to their service providers. • Provide guidelines for immediate steps if a device is lost or stolen, such as remotely wiping data.	• Users know how to report suspicious activities quickly. • Reduced risk of data compromise in case of device loss or theft.

Recover: Data Backup and Restoration	• Stress the importance of regular backups of financial data. • Train users on restoring data after a security incident. • Encourage users to review and update their security practices regularly.	• Regular data backups ensure data recovery after incidents. • Users learn from past incidents and continuously improve their security posture.
Analyse: Evaluate Threats and User Behaviour	• Assess specific threats to mobile financial services, such as phishing, malware, and unauthorized access. • Analyse user interactions with mobile financial services to identify common mistakes and risky behaviours.	• A comprehensive understanding of threats to mobile financial services. • Identification of areas where users need more awareness and training.

Function	Activities	Outcomes
Plan: Define Goals and Create Engaging Content	• Set clear goals for the cybersecurity awareness program. • Develop relevant and engaging content addressing specific security issues. • Choose effective channels to reach users, such as in-app notifications, SMS alerts, emails, and interactive tutorials.	• Defined goals help measure the success of the awareness program. • Engaging content ensures better user understanding and retention of security practices. • Effective communication channels reach a broad audience.

Train: Personalized Training Programs	• Develop personalized training programs tailored to individual user profiles. • Use interactive sessions, webinars, simulations, gamification, and scenario-based learning.	• Users receive personalized training that addresses their specific needs and risk levels. • Interactive and engaging training methods enhance user learning and application of security measures.
Reinforce: Embed Security Awareness in Daily Habits	• Implement techniques to keep users engaged and reinforce learned behaviours. • Send regular reminders and updates about security best practices. • Use ongoing challenges, quizzes, and refreshers to reinforce key security concepts. • Provide feedback on users' security behaviours and encourage improvements.	• Security awareness becomes part of users' daily routines. • Continuous engagement helps users maintain good security practices. • Users receive timely feedback and guidance to improve their security behaviours.

Source: Compiled by the Researcher

5.8. CHAPTER SUMMARY

In this chapter, the research findings and derived conclusions have been presented, offering insightful reflections based on the analysis of the survey results. The role of training and awareness in improving the security posture of users is undoubtedly very important. However, the survey results reveal a number of users struggling with basic security measures that can significantly safeguard their financial data. There is a need for immediate intervention based on these user challenges.

Based on these challenges, the author proposes a model to raise mobile security awareness and improve secure user behaviour when conducting mobile financial transactions. The model, known as the Adaptive Governance and Awareness Model (AGAM), combines NIST Cybersecurity and MediaPro Adaptive Awareness Frameworks in an integrated awareness model, thereby offering a comprehensive approach to cybersecurity for mobile financial services. Governance ensures alignment with organizational goals; identification and protection focus on securing assets; detection and response provide immediate incident handling; and recovery ensures that users are able to enjoy financial services after a cyber-attack. MediaPro's emphasis on analysis, planning, training, and reinforcement complements these technical measures by fostering a security-aware culture among users. This integrated

model demonstrates how adaptive awareness processes (MediaPro) enhance and support the core cybersecurity functions (NIST), creating a comprehensive and dynamic cybersecurity strategy. This holistic approach addresses both the technological and human aspects of cybersecurity, essential for protecting sensitive financial information.

Chapter 6: Recommendations and Conclusions

If we knew what it was, we were doing, it would not be called research, would it?

Albert Einstein

6.1. INTRODUCTION

This final chapter presents the research study's conclusions, examines the validation of the research, illustrates its contribution to the existing scientific knowledge, and culminates in proposing potential avenues for future research.

6.2. VALIDATION OF RESEARCH

This research employed desk research and qualitative and quantitative methodologies. Quantitative methodology was achieved using questionnaires administered among 1159 users of MFS and 23 information security professionals. Qualitative methodology was achieved through the study and observation of users and providers of MFS. The research employed a desktop research approach to gather valuable insights on best practices related to Cybersecurity training and awareness as well as potential cybersecurity topics.

The study aimed to address the lack of a framework that would guide training and awareness for users of mobile financial services. The presented model was formulated using the NIST Cybersecurity and MediaPro Adaptive Awareness frameworks as its foundation. The initial constructs of this model were derived from both the literature review and the analysis of the questionnaire results. The final model of user training awareness has been validated using statistical means.

The initial questionnaire was piloted with 200 users of MFS and 26 information security practitioners. The questionnaires were improved to reflect feedback from the pilot study. A final questionnaire was then distributed among 1170 users and 35 information security practitioners and MFS providers. Of the respondents, 54% were male, while females accounted for 46%. Additionally, most respondents were aged between 18–25 years, accounting for 43% of the respondents, while those aged 61 years and above accounted for 2.5% of the respondents.

6.3. ANALYSIS OF THE RESEARCH STUDY

An analysis of the research study is as follows:

i. **Chapter One:** This introductory chapter provides a comprehensive background to the study, outlining the research objectives, justifying the need for the study, and describing the study's design aimed at achieving the specified objectives.

ii. **Chapter Two:** In this chapter, an in-depth review of relevant literature is presented, establishing the foundational knowledge and context for the current study. The study began with a presentation on the developments within the financial sector, the automation path of financial services provision, the role of information systems in improving financial service delivery, the structure of mobile financial services, information security and privacy and their effects on mobile financial services, security theatre and how it impacts the overall information security posture, the gaps in Kenyan educational institutions that prepare professionals for information security roles, and finally, a presentation of how Security Education Training and awareness helps improve security behaviour.

iii. **Chapter Three:** This chapter presented the theoretical framework that underpinned this research. It justified the choice of the NIST cybersecurity and MediaPro Adaptive awareness framework.

iv. **Chapter Four:** This chapter elaborates on the research methodology adopted for the study, detailing the approach, data collection methods, and analytical techniques employed.

v. **Chapter Five:** This chapter delves into the analysis of the questionnaires utilised in the study and provides a comprehensive examination of the study's results and reflections.

vi. **Chapter Six:** The final chapter offers a conclusive summary of the research study, encompassing a synthesis of the findings, the study's contribution to both scientific knowledge and practical application, a candid exploration of its limitations, and recommendations for potential areas of future research.

6.4. RESEARCH CONTRIBUTION AND IMPLICATIONS FOR PRACTISE

The study tackled the problem of lacking a model for training users of mobile financial services. By examining the constructs of the NIST Cybersecurity and MediaPro Adaptive Awareness frameworks, the study developed an integrated model combining elements from both frameworks. The primary contribution of this research is the creation and establishment of the Adaptive Governance Awareness Model (AGAM), based on the NIST Cybersecurity and

MediaPro Adaptive Awareness frameworks. This model advances knowledge by outlining high-level constructs essential for the effective planning and management of cybersecurity awareness training programs.

The study validated that constructs from the NIST and MediaPro frameworks significantly enhance the security posture of mobile financial services (MFS) users. Although developed for MFS users, the final model is easily adaptable to any business environment. Additionally, government institutions can use this framework to boost information security awareness among users and the general public. Implementing AGAM can help government institutions strengthen their efforts to protect information assets and infrastructure, fostering trust and confidence among citizens when accessing government services through electronic and mobile channels.

Information security professionals facing challenges in persuading executive management to back information security training and awareness initiatives can now rely on this model as a valuable resource. By utilising AGAM, they can construct a compelling business case, effectively showcasing the benefits and value of such initiatives. This model serves as a guide, empowering these professionals to secure the necessary funding and obtain management buy-in, ultimately bolstering the organisation's overall cybersecurity posture.

Importantly, AGAM was designed with end-user accessibility and adaptability in mind. Its modular structure allows for diverse delivery methods tailored to varying literacy levels and access to technology. These include SMS-based alerts for users with basic phones, simplified infographics and animations for visual learners, mobile app tutorials for smartphone users, and face-to-face community-based workshops for those in rural or low-connectivity areas. Such practical adaptation mechanisms are critical for ensuring the model's usability across different segments of the population.

The framework also holds promise for broader application beyond the Kenyan context. Its core components—such as awareness, detection, response, and recovery—are sufficiently generic to be adapted to different regulatory environments, cultural norms, and technological infrastructures. For example, countries across Sub-Saharan Africa with similar mobile-first economies and information security gaps can modify AGAM to suit local conditions while maintaining its conceptual integrity. Thus, AGAM presents a scalable and transferable model for enhancing cybersecurity awareness in other emerging digital economies.

6.5. STUDY LIMITATIONS AND SUGESTIONS FOR FUTURE WORK

The respondents in the study were drawn from five counties due to time and resource constraints. If resources were available, the study would have been conducted in all 47 counties within Kenya.

The study's design was limited by its focus on collecting quantitative data. As a result, the data only pertained to the NIST Cybersecurity and MediaPro Adaptive Awareness variables, and no descriptive narrative data was gathered. While it is common practice to use quantitative data to analyse relationships between variables, this approach meant the results lacked detailed accounts of specific cybersecurity incidents and participants' personal reflections (Rahi, 2017; Young et al., 2016; Zeng et al., 2021)

This study's scope is restricted to the financial services industry. However, future research could expand its focus to encompass other sectors such as investment, insurance, and government services delivered through mobile channels. By conducting a comparative analysis across these various industries, researchers can gain valuable insights into the state of secure mobile behaviour among users. This broader examination will provide a more comprehensive understanding of information security practices and potential variations in secure mobile behaviour across different sectors.

Given the importance of real-world applicability, future studies should explore how AGAM can be implemented effectively across diverse user populations. This includes piloting delivery mechanisms suited for different literacy levels and technology access—such as SMS campaigns, visual storytelling tools, mobile-based interactive learning platforms, or in-person workshops led by trained facilitators. Evaluating the relative success of these methods can inform best practices for broad and inclusive deployment.

Furthermore, future work should examine how AGAM can incorporate continuous feedback from users to remain dynamic and responsive. Mechanisms such as periodic surveys, mobile-based user feedback forms, and community focus group discussions should be trialled to gather ongoing user insights. This feedback can then be systematically analysed to identify evolving awareness needs and refine the model's delivery content and approach.

Finally, to assess AGAM's scalability and cross-cultural relevance, comparative studies across countries with similar mobile financial ecosystems are recommended. Such research should identify the modifications necessary for localising AGAM to different socio-cultural,

infrastructural, or regulatory settings, thereby enhancing its global relevance and strategic impact.

6.6. CONCLUSSION

The AGAM model was derived from a combination of constructs of NIST cybersecurity and MediaPro Adaptive awareness frameworks and the findings obtained from the questionnaire. However, it holds potential for further development and extension. To enhance the model's effectiveness, more in-depth analysis of the relationships between its constructs may be required. By conducting additional research, researchers can gain a better understanding of these relationships, leading to improvements in the model's structure and application. This ongoing development and refinement process will ensure that the AGAM continues to be a valuable and adaptable tool for information security training and awareness initiatives.

References

Afriyie, B. S. (2022). Exploring Methods Cybersecurity Managers Need to Implement to Minimize Cyber-Frauds in Mobile Money Services in Ghana . *Doctoral dissertation*. Colorado Technical University.

Ahirrao, K., & Jethani, V. (2014). A Security Framework on SIM Based Authentication Technique for Mobile Financial Services. Retrieved April 19, 2022, from https://www.researchgate.net/publication/350853795_A_Security_Framework_on_SIM_Based_Authentication_Technique_for_Mobile_Financial_Services/citation/download

Ahola, M. (2021). *The Role of Human Error in Successful Cyber Security Breaches*. Retrieved April 19, 2022, from USecure: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (2005). The Influence of Attitudes on Behavior. *Handb. Attitudes*, 173–222.

Akbulut, Y. (2007). *Implications of Two Well-Known Models for Instructional Designers in Distance Education: Dick-Carey versus Morrison-Ross-Kemp.* .

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3).

Al-Delayel, A. S. (2022). Security Analysis of Mobile Banking Application in Qatar.

Al-Doghan, M. A., & Mirzaliev, S. (2024). Cybersecurity Awareness and Digital Banking Adoption: Exploring the Moderating Impact of Digital Literacy. *International Journal of Economics and Finance Studies, 16*(3), 34-58. doi:10.34109/ijefs.202416303

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2021). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*.

Al-Haydary, M. K., & Majeed, B. H. (2021). Impact of ASSURE Model on Mathematical Correlation and Achievement in Mathematics. *European Journal of Humanities and Educational Advancements (EJHEA), 2*(11), 62-68.

Ali, G., Ally, D., & Elikana, S. A. (2020). Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda . *11*(6), 309. doi:https://doi.org/10.3390/info11060309

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing, 25*(5), 829-841.

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security, 100*.

Alshehri, A., Alghamdi, A., & Jameel, F. (2023). An adaptive cybersecurity training framework for the education of social media users at work. *Applied Sciences, 13*(17). Retrieved July 18, 2025, from https://www.mdpi.com/2076-3417/13/17/9595

Alsmadi, I., Burdwell, R., Aleroud, A., Wahbeh, A., Al-Qudah, M., & Al-Omari, A. (2018). Security and Access Controls: Lesson Plans. In *Practical Information Security* (pp. 53-71). Springer, Cham. doi:https://doi.org/10.1007/978-3-319-72119-4_3

Altamimi, S. (2022). Investigating and mitigating the role of neutralisation techniques on information security policies violation in healthcare organisations. *Doctoral dissertation, University of Glasgow*.

Ambore, S., Richardson, C., Dogan, H., Apeh, E., & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology, 1*(3-4), 202-224.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. *Computers in Human Behavior, 114*.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems, 147*.

Asad, M., Hassan, R., & Sherwani, F. (2014). Instructional models for enhancing the performances of students and workforce during educational training. *Academia Arena, 6*(3), 27-31.

Ayyash, M. M. (2022). A Thorough Analysis of the Perceived Risk and Customer Acceptance of Mobile Banking Apps. *International Conference on Business and Technology* (pp. 35-49). Springer, Cham.

Aziz, A., & Naima, U. (2021). Rethinking digital financial inclusion: Evidence from Bangladesh. *Technology in Society, 64*.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?

Bajracharya, J. (2020). Instructional Design and Models: ASSURE and Kemp. *Journal of Education and Research, 9*, 1-8.

Barbu, C. M., Florea, D. L., Dabija, D. C., & Barbu, M. C. (2021). Customer experience in fintech. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(5), 1415-1433.

Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in Financial Sector Development. *CGAP Background Documents*.

Beck, E., Goin, M. E., Ho, A., Parks, A., & Rowe, S. (2021). Critical digital literacy as method for teaching tactics of response to online surveillance and privacy erosion. *Computers and Composition, 61*.

Bergman, M. M. (2008). *Advances in Mixed Methods Research:Theories and Applications (1st ed.).* London: Sage.

Bett, R. (2020, July 4). *Enhance digital security awareness for users*. Retrieved April 24, 2022, from Nation: https://nation.africa/oped/opinion/Enhance-digital-security-awareness-for-users/440808-4523228-34i23kz/index.html

Bhana, A., & Ophoff, J. (2022). Security Fatigue: A Case Study of Data Specialists. *International Symposium on Human Aspects of Information Security and Assurance* (pp. 275-284). Springer, Cham.

Bharati, S., & Suguna, J. (2014). A Conceptual Model To Understand Information Security Awareness. *International Journal of Engineering Research & Technology (IJERT), 3*(8).

Bhardwaj, A., & Kaushik, K. (2022). Predictive Analytics-Based Cybersecurity Framework for Cloud Infrastructure. *International Journal of Cloud Applications and Computing (IJCAC), 12*(1), 1-20.

Borich, G. (1979). Implications for developing teacher competencies from process-product research. *Journal of Teacher Education, 30*(1), 77-86.

Bosamia, M., & Patel, D. (2019). Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *International Journal of Computer Sciences and Engineering, 7*, 810-817. doi:10.26438/ijcse/v7i1.810817

Boston Consulting Group (BCG). (2020). *Global Payments 2020: Fast Forward into the Future*. Retrieved March 23, 2022, from https://www.bcg.com/publications/2020/payments-industry-fast-forwards-into-the-future

Branch, R. M., & Gustafson, K. L. (1998). *Re-visioning models of instructional development.* UK: Upper Saddle River.

Brecht, D. (2019, April 15). *The components of top security awareness programs*. Retrieved April 24, 2022, from https://resources.infosecinstitute.com/topic/components-top-security-awareness-programs/#gref

Buckbee, M. (2020, September 28). *Data Privacy Guide: Definitions, Explanations and Legislation*. Retrieved April 20, 2021, from Varonis: https://www.varonis.com/blog/data-privacy

Burgess, M. (2020, March 24). *What is GDPR? The summary guide to GDPR compliance in the UK*. Retrieved April 20, 2021, from Wired: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

Carbo-Valverde, S. H., & Rodriguez-Fernandez, F. (2003). Effects on the banking system and the economy. *Electronic Payments*, 88(1), 41-50.

Central bank of Kenya (CBK). (2017, August). *CBK Guidance Note on Cybersecurity*. Retrieved June 19, 2021, from CBK:

https://www.centralbank.go.ke/uploads/banking_circulars/634077191_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf

Central Bank of Kenya (CBK). (2019, July). *Legislation and Guidelines.* Retrieved April 20, 2022, from CBK Website: https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf

Central Bank of Kenya (CBK). (2020). *Bank Supervision & Banking Sector Reports.* Central Bank of Kenya. Retrieved April 10, 2022, from https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/468154612_2020%20Annual%20Report.pdf

Central Bank of Kenya (CBK). (2021). *CBK Annual Reports.* Retrieved March 23, 2022, from https://www.centralbank.go.ke/uploads/cbk_annual_reports/569264497_Annual%20Report%202020-2021.pdf

Chai, W. (2021). Confidentiality, Integrity and Availability (CIA triad). Retrieved April 20, 2022, from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program,. *Journal of Cybersecurity, 8*(1).

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access, 10*, pp. 85701-85719.

Ching, H. L., & Ellis, P. (2004). What factors drive e-commerce adoption? *Journal of Marketing Management,*, 20(3-4), 409-429.

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review, 40*.

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security, 113*.

Christopher, A. (2011, November 13). *Instructional Designer's Job Aids. Instructional Design Process*. Retrieved December 15, 2021, from MRK Job Aids: https://issuu.com/avchristopher/docs/christopher_mrk_jobaids_final3

CIO Africa. (2017, June 23). *ESET announces free online cybersecurity awareness training for businesses in Kenya*. Retrieved April 24, 2022, from CIO Africa: https://cioafrica.co/eset-announces-free-online-cybersecurity-awareness-training-for-businesses-in-kenya/

CISCO. (2021). *Cisco Cybersecurity Reports.* Cisco. Retrieved April 24, 2022, from https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Cofense. (2021). *Annual State of Phishing Report.* Cofense. Retrieved April 19, 2022, from https://cofense.com/wp-content/uploads/2021/02/cofense-annual-report-2021.pdf

Communications Authority of Kenya (CAK). (2021). *Sector Statistics Report.* Retrieved March 23, 2022, from https://www.ca.go.ke/wp-content/uploads/2021/12/Sector-Statististics-Report-Q1-2021-2022.pdf

Cooper, D. R., & Schindler, P. S. (2008). *Business Research Methods. 10th ed.* . New York.

Cranfield, D., Venter, I., Blignaut, R., & Renaud, K. (2020). Smartphone Security Awareness, Perceptions and Practices: A Welsh Higher Education Case Study. 3014-3023.

Creswell, J. W., & Plano-Clark, V. L. (2007). *Designing and Conducting Mixed Methods Research.* ThousandOaks, California: Sage Publications.

Crowther, D., & Lancaster, G. (2012). *Research methods:* . Routledge.

Cukier, M. (2007, February 9). *Study: Hackers Attack Every 39 Seconds*. Retrieved from University of Maryland: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Cybint. (2020, December 23). *Cyber Security Facts and Stats*. Retrieved April 20, 2022, from Cybint Solutions: https://www.cybintsolutions.com/cyber-security-facts-stats/

Cytonn. (2019, February 17). *Fintech Impact on Kenya's Financial Services Industry*. Retrieved from Cytonn: https://www.cytonn.com/topicals/fintech-impact-on-kenyas-financial-services-industry

D'Angelo, T., Bunch, J. C., & Thoron, A. (2018). Instructional design using the Dick and Carey systems approach. *AEC632, the Department of Agricultural Education and Communication*.

Daly, J. (2022). *12 Essential Security Awareness Training Topics for 2022*. Retrieved April 24, 2022, from USecure: https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020

Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

Davies. (2002). *A History of Money: From ancient times of the the present day.* University of Wales Press.

de Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *ScienceDirect, 34*(1), 1-14. Retrieved July 18, 2025, from https://doi.org/10.1016/j.giq.2017.02.007

Dick, W., Carey, L., & Carey, J. O. (2005). *The systematic design of instruction.* Boston, Massachusetts: Pearson/Allyn and Bacon.

E, A. (n.d.). A qualitative study of users' view on information security. In A. E, *In computer & Security 26* (pp. 276-289).

Ekran. (2022, April 6). *Best Practices to Prevent Cyber Attacks*. Retrieved August 18, 2022, from Ekran: https://www.ekransystem.com/en/blog/best-cyber-security-practices

Equity Bank. (2020). *Financial Reports*. Retrieved April 24, 2021, from Equity Bank: https://investor.equitybank.com/financials/financial-reports

Ernest & Young. (2019). *Global FinTech Adoption Index.* Ernest & Young. Retrieved April 23, 2022, from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-global-fintech-adoption-index-2019.pdf

Ernst & Young. (2021). *Global Information Security Survey 2021*. Retrieved March 2022, 2022, from https://www.ey.com/en_vn/ey-global-information-security-survey-2021

ESET. (2017, May 1). *ESET survey reveals nearly one in three Americans receives no cybersecurity training in the workplace*. Retrieved April 1, 2022, from https://www.eset.com/us/about/newsroom/corporate-blog/eset-survey-reveals-nearly-one-in-three-americans-receives-no-cybersecurity-training-in-the-workplac/

European Union Agency for Cybersecurity (ENISA). (2021). *ENISA Threat Landscape 2020.* ENISA. Retrieved April 24, 2022, from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020

Fakiya. (2023). *A credit Referencing Agency.*

Farooq, M. S., Munir, K., Alvi, A., & Omer, U. (2022). Design of a Substitution Box using a Novel Chaotic Map and Permutation.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics*, *1139*(1), 12098.

Fauser, M., Henry, D., & Norman, L. (2006). *Comparison of alternative instructional design model.* Hoboken, NJ: John Wiley & Son, Inc.

Feyen, E., Frost, J., Natarajan, H., & Rice, T. (2021). What does digital money mean for emerging market and developing economies? *In The Palgrave Handbook of Technological Finance*, 217-241.

Finacial Services Deepening (FSD). (2021). *FinAccess Household Surveys.* Retrieved May 10, 2022, from https://www.fsdkenya.org/category/finaccess/finaccess-household-surveys/

Forest, E. (2016). *Kemp Design Model*. Retrieved April 23, 2020, from http://educationaltechnology.net/kempdesignmodel/

Furst, K. L., & Nolle, D. E. (2000). *Internet banking: Developments and prospects.*

Gartner. (2019, October 19). *Is the Cloud Secure?* Retrieved October 14, 2021, from Gartrner: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Gauthier, J. (2005). Moving Closer to a Universal Declaration of Ethical Principles for Psychologists: Progress Report and Draft. .

Gay, L. R. (1992). *Educational research.* New York: Maxwell Macmillan.

Gebel, G. (2019, January 16). *Critical data security trends for 2019 and beyond*. Retrieved December 19, 2021, from IT Pro Portal: https://www.itproportal.com/features/critical-data-security-trends-for-2019-and-beyond/

Giles, M. (2013, February 7). *The Kemp ID Model*. Retrieved April 24, 2021, from https://www.slideshare.net/lindamgiles/kemp-id-modelpresmgiles-16411696

Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for likert-type scales. *2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education.* Retrieved August 21, 2024, from http://pioneer.chula.ac.th/~ppongsa/2900600/LMRM08.pdf

Government of Kenya. (2019). *Data Protection Act. accessed on.* Retrieved March 2, 2022, from https://www.odpc.go.ke/dpa-act/

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*(181), 59-66.

Grundy, S., & Kemmis, S. (1981). Educational Action Research in Australia: The State of the Art. *Australian Association for Research in Education.*

GSMA. (2021). *State of the Industry Report on Mobile Money.* Retrieved May 10, 2022, from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money-2021_Full-report.pdf

GTISC. (2022). *Emerging Cyber Threats Report 2021*. Cyber Threat Report, Atlanta. Retrieved April 3, 2022, from http://www.gtisc.gatech.edu/pdf/cyberThreatReport2021.pdf

Gup, B. E. (2011). *Bank failures in the major trading countries of the world:Causes and Remedies.* Greenwood Publishing Group.

Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. *In Research anthology on artificial intelligence applications in security* (pp. 1960-1977). IGI Global.

Haider, H. (2018). Innovative financial technologies to support livelihoods and economic outcomes.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* (Vol. 6). Upper Saddle River, NJ: Pearson Prentice Hall.

Hakami, M., & Alshaikh, M. (2022). Identifying Strategies to Address Human Cybersecurity Behavior: A Review Study. *International Journal of Computer Science & Network Security, 22*(4), 299-309.

Ham, J. V. (2021). Toward a Better Understanding of "Cybersecurity" Digital Threats: Research and Practice. *2*(3), 1-3.

Hanley, M. (2009). *Discovering Instructional Design 11: The Kemp Model*. Retrieved April 25, 2020, from http://elearningcurve.blogspot.com.tr/2009/06/discovering-instructional-design-11.html

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Information Security and Applications, 58*.

He, W., Tian, X., & Shen, J. (2015). Examining security risks of mobile banking applications through blog mining. *CEUR Workshop Proceedings*, (pp. 103-108).

Heinich, R., Molenda, M., D., R. J., & Smaldino, S. E. (2002). *Instructional media and technologies for learning.* New Jersey: Merrill Prentice Hall.

Herath, T. C., Herath, H. S., & Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. . *Information Systems Frontiers*, 1-41.

Hight, S. D. (2017). The importance of a security, education, training and awareness program (2005). Raleigh.

Hu, S., Hsu, C., & Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems, 62*(4), 752-764.

Hudgens, J. (2017, April 24). *Top Tips for Developing Effective Security Awareness and Training Programs*. Retrieved December 19, 2021, from Pratum: https://www.pratum.com/blog/369-top-tips-for-developing-effective-security-awareness-and-training-programs

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyo, 7*(3).

IBM. (2022). *Cost of a Data Breach Report 2021*. IBM. Retrieved April 20, 2022, from https://www.ibm.com/downloads/cas/OJDVQGRY

IBM. (2022). *IBM Cyber Security Intelligence Index Report.* IBM. Retrieved August 20, 2022, from https://www.ibm.com/downloads/cas/ADLMYLAZ

IBM. (2022, August 10). *User security responsibilities*. Retrieved April 10, 2022, from IBM Website: https://www.ibm.com/docs/en/aix/7.2?topic=administration-user-security-responsibilities

Infosec. (2017, August 29). *Security Awareness Statistics*. Retrieved June 12, 2022, from Infosec Institute: https://resources.infosecinstitute.com/topic/security-awareness-statistics/

Interpol. (2021). *African Cyberthreat Assessment Report.* Interpol. Retrieved June 20, 2022, from https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf

Iser, B., & Brandtweiner, R. (2022). Role of awareness to prevent personal disasters: Reducing the risks of falling for phishing by strengthening user awareness. . *WIT Transactions on The Built Environment, 207*, 79-88.

ISO/IEC 27002. (2022). *Information security, cybersecurity and privacy protection — Information security controls.* Retrieved June 10, 2022, from ISO/IEC 27002:2022: https://www.iso.org/standard/75652.html

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis . *Complex & Intelligent Systems, 7*(5), 2157-2177.

Jelen, S. (2019, November 12). *Security Theater: Are You Feeling Secure or Actually Being Secure?* Retrieved August 19, 2022, from SecurityTrails: https://securitytrails.com/blog/security-theatre

Jennings, M. (2022). *Top data breaches and cyber attacks of 2022*. Retrieved September 16, 2022, from Techradar: https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher, 33*(7), 14–26.

Johnson, R., & Christensen, L. (2008). *Educational research: Quantitative, qualitative and mixed approaches.* Thousand Oaks, California: SAGE.

JT Force. (2020). Security and Privacy Controls for Information Systems and Organizations. *NIST Publications*. Retrieved April 19, 2022, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Kaibiru, R. M., Karume, S. M., Kibas, F. K., & Onga'nyo, M. L. (2023, April). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. *Journal of Information Security, 14*(2). doi:10.4236/jis.2023.142009

Kaminski, P., Rezek, C., Richter, W., & Sorel, M. (2017, January 31). *Protecting your critical digital assets: Not all systems and data are created equal*. Retrieved April 20, 2022, from McKinsey: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/protecting-your-critical-digital-assets-not-all-systems-and-data-are-created-equal

Kaspersky. (2021). *Kaspersky Security Bulletin 2020: Statistics.* Kaspersky. Retrieved April 24, 2022, from https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

Kaspersky. (2022, February 21). *2021 Mobile threats report: cybercriminals forego low hanging fruit to go after banking and gaming*. Retrieved April 27, 2022, from Kaspersky: https://www.kaspersky.com/about/press-releases/2022_2021-mobile-threats-report-cybercriminals-forego-low-hanging-fruit-to-go-after-banking-and-gaming

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*.

Kim, L. (2022). Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information. *Nursing Informatics*, 391-410.

King, N. (2021, March 2). *The importance of information security*. Retrieved April 3, 2022, from Vigilant Software: https://vigilantsoftware.co.uk/blog/the-importance-of-information-security

Kiruthika, R., & Chakravarthy, P. D. (2019). Correlating information security awareness with human psychology. *International Journal of Production Technology and Management (IJPTM), 10*(1), 144-155.

Klahr, R., Shah, J., Sheriffs, P., Tossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017. (Main report).*

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*.

KPMG. (2019). *Global Banking Fraud Survey*. Retrieved March 24, 2022, from https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf

Kritzinger, E., & Smith, E. (2008). *Five Steps to Effective Security Awareness* . Forrester Research.

Krutz, R. L., & Russell, D. (2001). *The CISSP Prep Guide.* New York: John Wiley & Sons, Inc.

Kurt, S. (2016, December 12). *Kemp Design Model*. Retrieved from Education Technology: https://educationaltechnology.net/kemp-design-model/

Lagarde, C. (2018). Estimating Cyber Risk for the Financial Sector.

Larios-Vargas, E., Elazhary, O., Yousefi, S., Lowlind, D., Vliek, M. L., & Storey, M. A. (2022). DASP: A Framework for Driving the Adoption of Software Security Practices.

Leedy, P., & Ormrod, J. (2010). *Practical research: planning and design. 9th ed.* Upper Saddle River, NJ: Merrill.

Li, Y. (2016). *Expatriate Manager's Adaption and Knowledge Acquisition: Personal Development in Multi-National Companies in China.* Springer Publications.

Lohrmann, D. (2014, March 9). *Ten Recommendations for Security Awareness Programs*. Retrieved April 24, 2022, from Government Technology: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/ten-recommendations-for-security-awareness-programs.html

Madhav, A. V., & Tyagi, A. K. (2022). The world with future technologies (Post-COVID-19): Open issues, challenges, and the road ahead. *Intelligent Interactive Multimedia Systems for e-Healthcare Applications* (pp. 411-452). Singapore: Springer.

Makin, P. (2018, November 15). *Cybersecurity for Mobile Financial Services: A Growing Problem*. Retrieved June 20, 2022, from CGAP: https://www.cgap.org/blog/cybersecurity-mobile-financial-services-growing-problem

Malero, A. (2015). Measuring Security Awareness on Mobile Money Users in Tanzania. *International Journal of Engineering Trends and Technology, 20*, 44-47.

Malhotra, N. (2004). *Marketing Research: An applied orientation.* Upper Saddle River, NJ: Prentice Hall.

Mann, C. (2011, December 20). *Smoke Screening*. Retrieved April 16, 2021, from Vanity Fair: https://www.vanityfair.com/culture/2011/12/tsa-insanity-201112

Mater, W., Matar, N., Alismaiel, O. A., Al Moteri, M. A., Al Youssef, I. Y., & Al-Rahmi, W. M. (2021). Factors influencing the intention behind mobile wallet adoption: Perceptions of university students . *Entrepreneurship and Sustainability Issues, 9*(1), 447.

Maurushat, A. (2022). The legal obligation to provide timely security patching and automatic updates. *International Cybersecurity Law Review*, 1-29.

Mayer, T. (2017). How ATMs changed banking and the world. *The International Journal of Bank Marketing,*, 35(2), 142-160.

Mazer, R. (2018). Emerging data sharing models to promote financial service innovation: Global trends and their implications for emerging markets.

Mazzarolo, G., Casas, J. C., Jurcut, A. D., & Le-Khac, N. A. (2021). Protect against unintentional insider threats: The risk of an employee's cyber misconduct on a social media site. *Cybercrime in Context* (pp. 79-101). Springer, Cham.

McBride, N., & Liyala, S. (2021). Memoirs from Bukhalalire: a poetic inquiry into the lived experience of M-PESA mobile money usage in rural Kenya. *European Journal of Information Systems*, 1-22.

McCutcheon, G., & Jurg, B. (1990). *Alternative Perspectives on Action Research* (Vol. 24). Summer: McGraw-Hill Publishing Company Limited.

McIlwraith, A. (2021). *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness* (2 ed.). Routledge. doi:https://doi.org/10.4324/9780429281785

MediaPro. (2016). Adaptive Awareness Framework. *NIST FISSEA Presentation.* NIST. Retrieved from https://csrc.nist.gov/CSRC/media/Presentations/FISSEA-2016-Conference-Presentation-Adaptive-Awa/images-media/FISSEA_Pendergast_MediaPro_Adaptive_Awareness_Framework_Resources-Wed0115.pdf

Melnikovas, A. (2018). Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies. *Journal of Futures Studies, 23*(2), 29-44.

Michalsons. (2021). *Information Security Law*. Retrieved April 20, 2022, from Michalsons: https://www.michalsons.com/focus-areas/information-technology-law/information-security-law

Mingers, J. (2006). *Realising Systems Thinking: Knowledge and Action in Management Science.* New York: Springer.

Morrison, G. R., Ross, S. M., Kemp, J. E., & Kalman, H. (2010). *Designing effective instruction.* Hoboken, New Jersey: John Wiley & Sons.

Morrison, G., Ross, S., Kalman, H., & Kemp, J. (1998). *Designing Effective Instruction.* New Jersey: Prentice Hall.

Mpofu, F. Y. (2022). Industry 4.0 in Financial Services: Mobile Money Taxes, Revenue Mobilisation, Financial Inclusion, and the Realisation of Sustainable Development Goals (SDGs) in Africa. *Sustainability, 14*(14).

Mwangi, K., & Kasamani, B. (2017). A Universal Mobile Money Transfer Platform. *International Journal of Computer Applications, 175*(6). doi:https://www.ijcaonline.org/archives/volume175/number6/mwangi-2017-ijca-915595.pdf

Myriad Group. (2019). *Kenya Fraud Report: Digital & mobile finacial transaction fraud 2018.* Myriad Group. Retrieved April 19, 2022

Nakamoto, S. (2008). *A peer-to-peer electronic cash system.* Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A. B., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies:*. Princeton University Press.

National Institute of Standards and Technology. (n.d.). Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nayak, J. K., & Singh, P. (2021). Fundamentals of research methodology problems and prospects.

Nduati, H. (2018). *Cyber Security in Emerging Finacial Markets.* CGAP. Retrieved April 20, 2022, from https://www.findevgateway.org/sites/default/files/publications/files/cybersecurity_in_emerging_markets_06-30_0.pdf

Ndung'u, N., & Oguso, A. (2021). Financial sector development and financial inclusion in Africa: Gaps, Challenges and Policy options. *Inclusive Financial Development*, 28-51.

Nelito. (2021). *Everything you need to know about mobile money in kenya.* Retrieved March 23, 2022, from https://www.nelito.com/blog/everything-you-need-to-know-about-mobile-money-in-kenya.html

NetScouts. (2018). *Dawn of the TerrorBIT era NETSCOUT threat intelligence*. Retrieved June 14, 2021, from NetScouts: https://www.netscout.com/sites/default/files/2019-02/SECR_001_

Neuman, W. (2000). *Social Research Methods.* . Needham Heights, MA : Allyn & Bacon.

Ngahu, C., Kibera, F., & Kobonyo, P. (2022). Influence of interactional justice strategy on recovery satisfaction among customers of mobile money services in Kenya. *Journal of Marketing and Consumer Research, 22*, 1-10. Retrieved from http://www.iiste.org/Journals/index.php/JMCR/article/view/33118

NIST. (2014, July 25). *special Publication 800-12: An Introduction to Computer Security: The NIST Handbook.* Retrieved April 24, 2022, from NIST Computer Security Response Center: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter13.html

NIST. (2018). Retrieved from Framework for Improving Critical Infrastructure Cybersecurity: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2021, September 21). *Building a Cybersecurity and Privacy Awareness and Training Program.* Retrieved April 24, 2022, from NIST Computer Security Resource Centre: https://csrc.nist.gov/publications/detail/sp/800-50/rev-1/draft

NIST. (2021, May 12). *Cybersecurity Framework*. Retrieved April 20, 2022, from NIST: https://www.nist.gov/cyberframework/online-learning/five-functions

Nobles, C. (2022). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA–Journal of Business and Public Administration*, *13*(1), 49-72.

Obizoba, C. (2015). Instructional design models—framework for innovative teaching and learning methodologies. *The Business and Management Review*, *6*(5).

Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computers & Security, 108*.

O'Leary, D. (2020, September 3). *Best practices for building an effective security awareness program*. Retrieved April 24, 2022, from SHI: https://blog.shi.com/cybersecurity/security-awareness-training-best-practices/

Oluwole, V. (2022, May 10). *Kenya's mobile money transactions surge by 63% in 2021 — report*. Retrieved June 14, 2022, from Business Insider Africa: https://africa.businessinsider.com/local/markets/kenyas-mobile-money-transactions-surge-by-63-in-2021-report/tmkw1rn

Ombati, V. O., Ogutu, M., & Chege, S. (2021). Digital literacy and cyber hygiene among rural populations in Kenya. *International Journal of ICT Research in Africa and the Middle East*, *10*(1), 45-58. Retrieved July 18, 2025, from https://doi.org/10.4018/IJICTRAME.2021010103

Otieno, D. (2021, January 6). *Banks need to do more to counter rising fraud cases in Kenya*. Retrieved March 24, 2022, from tech-ish: https://tech-ish.com/2021/01/06/rising-fraud-banks-kenya/

P.Tobin. (2011).

Packer, P. (2022). *The Top 6 Most Common Security Concerns with Mobile Banking Consumers*. Retrieved April 20, 2022, from Flexcutech: https://blog.flexcutech.com/blog/the-top-6-most-common-security-concerns-with-mobile-banking-consumers

Pandey, P., & Pandey, M. M. (2021). *Research methodology tools and techniques.* Bridge Centre.

Patel, S. (2015, July 15). *The research paradigm – methodology, epistemology and ontology – explained in simple language*. Retrieved April 24, 2022, from Dr Salma Patel: https://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language/

Pawlicka, A., Choraś, M., & Pawlicki, M. (2021). The stray sheep of cyberspace aka the actors who claim they break the law for the greater good. *Personal and Ubiquitous Computing, 25*(5), 843-852.

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). Work-in-Progress--Understanding motivations and characteristics of financially-motivated cybercriminals.

Pegueros, V. (2013, January 4). *Security of Mobile Banking and Payments*. Retrieved March 20, 2022, from SANS Institute reading Site: https://www.sans.org/white-papers/34062/

Pew Research Center. (2019). *2018 Global Attitudes Survey*. Pew Research Center. Pew Research Center. Retrieved April 24, 2022, from https://www.pewresearch.org/global/2019/03/04/u-s-german-relations-methodology-spring-2018-global-attitudes-survey/

Platt, J. L. (2008). The Efficacy of an Electronic Performance Support System as a Training Tool for Online Faculty. *Dissertation for doctorate degree*. Iowa State University, Iowa. Retrieved April 25, 2020, from https://books.google.com.tr/books?id=ImcRyPLmtrAC&lpg=PA165&ots=rzxT0ddqhM&dq=layers%20of%20kemp%20morrison%20ross&hl=tr&pg=PP1#v=onepage&q=layers%20of%20kemp%20morrison%20ross&f=false

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021). The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review. *Advances in Security, Networks, and Internet of Things*, (pp. 377-395).

Porup, J. (2020, May 27). *5 examples of security theater and how to spot them*. Retrieved December 4, 2021, from CSO: https://www.csoonline.com/article/3544293/5-examples-of-security-theater-and-how-to-spot-them.html

Pramod, D. (2024). Gamification in cybersecurity education; a state-of-the-art review and research agenda. *Journal of Applied Research in Higher Education*. Retrieved from https://doi.org/10.1108/JARHE-02-2024-0072

PwC. (2021). *Financial Services Technology 2020 and Beyond: Embracing disruption.* PwC. Retrieved April 24, 2022, from https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf

Quagliata, K. (2011). Impact of Security Awareness Training Components on Perceived Security Effectiveness . *Information Systems Audit and Control Association, 4*.

Quinn, S. &., & Roberds, W. (2009). An economic explanation of the early banknote. *Journal of Monetary Economics,*, 56(5), 835-850.

Rayanto, Y. H., & Supriyo, S. (2021). Teaching Classroom Management Subjects Through the Implementation of Assure Model Instructional Design. *ELT Worldwide: Journal of English Language Teaching, 8*(2), 403-408.

Razack, Y. (2022). A Security Awareness Program for PCI DSS Compliance: Implementation and Legal and Ethical Issues to Be Considered. *Information Systems Audit and Control Association*.

Reiser, R. A., Reiser, R. A., & Dempsey, J. V. (2011). *Trends and issues in instructional design and technology* . Boston: Pearson.

Rogoff, K. S. (2017). *The curse of cash: How large-denomination bills aid crime and tax evasion and constrain monetary policy.* Princeton University Press.

Ross, B., Douglas, A., & Janos, B. (2016). The Evolution of Fintech: A New Post-Crisis Paradigm? *Georgetown Journal of International Law., 47*(10), 1271-1319.

Russel, C. (2020). Security Awareness - Implementing an Effective Strategy.

Russel, C. (2020). Security Awareness: Implementing an Effective Strategy.

Sabillon, R. (2022). The Cybersecurity Awareness Training Model (CATRAM). *Research Anthology on Advancements in Cybersecurity Education* (pp. 501-520). IGI Global.

Salo-Lahti, M. (2022). Good or Bad Robots? Responsible Robo-Advising. *European Business Law Review, 33*(5).

Saunders, M., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students . 4th Edition* . Edinburgh Gate, Harlow: Financial Times Prentice Hall.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students.* New York: Pearson.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students.* England: 44 Pearson Education Limited .

Schiffman, L. G., & Kanuk, L. L. (1997). *Consumer Behaviour.* London: Prentice Hall.

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and Consequences of Data Breaches: A Systematic Review. *Information & Management*.

Schneier, B. (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* Copernicus Books.

Security Magazine. (20117, February 10). *Hackers Attack Every 39 Seconds*. Retrieved April 10, 2022, from Security: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds

Seels, B. B., & Richey, R. C. (1994). *Instructional technology: the definition and domains of the field.* Seven Fountains, Virginia: AAH Graphics.

Sekaran, U., & Bougie, R. (2010). *Research Methods for Business:A skill Building Approach.* United Kingdom: John Wiley& Sons Ltd.

Senanayake, J., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., & Piras, L. (2022). Android Source Code Vulnerability Detection: A Systematic Literature Review. . *ACM Computing Surveys (CSUR)*.

Shachmurove, N. C., & McCulloch, W. (2021). Health Care Companies Face Financial Strain from Data Breaches. *American Bankruptcy Institute, 40*(8), 20-52.

Shé, C. N., Farrell, O., Brunton, J., & Costello, E. (2022). Integrating design thinking into instructional design: The OpenTeach case study. *Australasian Journal of Educational Technology, 38*(1), 33-52.

Simon. (2021).

Smaldino, S. (2006). *Instructional Technology and Media for Learning.* UK; Upper Saddle River.

Sobers, R. (2022, July 8). *166 Cybersecurity Statistics and Trends*. Retrieved August 17, 2022, from Varonis: https://www.varonis.com/blog/cybersecurity-statistics

Sonowal, G. (2022). Training Methods for Phishing Detection. *Phishing and Communication Channels* , (pp. 137-152). A Press, Berkeley.

Spremić, M., & Šimunic, A. (2018). Cyber security challenges in digital economy. *In Proceedings of the World Congress on Engineering. 1*, pp. 341-346. Hong Kong, China:: International Association of Engineers.

Srinivasan, J. (2021). The social meaning of mobile money. Data-centric Living: Algorithms, Digitization and Regulation.

Steadman Group. (2007). *Financial Access in Kenya.* FSD Kenya. Retrieved October 2022, from https://www.fsdkenya.org/finaccess/financial-access-in-kenya-results-of-the-2006-national-survey/

Steinmetz, K. F., Knight, T., & McCarthy, A. L. (2022). Organizational characteristics associated with vulnerability to social engineering deception: A qualitative analysis. Victims & Offenders. *17*(3), 421-438.

Stringer, E. (1999). *Action Research: A handbook for Practitioners* (2 ed.). Newbury Park.

Subramanian, S. (2021, February 17). *Rethinking Information Security Awareness Strategies*. Retrieved April 19, 2022, from ISACA: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/rethinking-information-security-awareness-strategies

Suradika, A., Winata, W., Wicaksono, D., & Husainah, N. (2022). Instructional Development of Introduction to Statistics Based On Dick And Carey's Model: A Study At The Faculty Of Economics And Business, Muhammadiyah University, Jakarta. *The Social Perspective Journal*, *1*(2), 111-127.

Surf. (2022). *Mobile Banking App Security Issues: Main Threats And How To Avoid Them*. Retrieved from Surf: https://surf.dev/mobile-banking-app-security-issues

Susanto, H. (2021). Revealing Cyber Threat of Smart Mobile Devices within Digital Ecosystem: User Information Security Awareness. *Data Integrity and Quality.* IntechOpen.

Sutherland, L. (2016, March 31). *Know Your Enemy: Understanding the Motivation Behind Cyberattacks*. Retrieved April 24, 2022, from Security Intelligence: https://securityintelligence.com/know-your-enemy-understanding-the-motivation-behind-cyberattacks/

SWIFT. (n.d.). *History of SWIFT.* Retrieved from https://www.swift.com/about-us/history

Swinnen, E. (2020, April 01). *The Ultimate Data Privacy Guide for Banks and Financial Institutions*. Retrieved March 7, 2022, from Ng Data: https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/

Talib, S., Clarke, N., & Furnell, S. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *2010 International Conference on Availability, Reliability and Security.*

The East African. (2021, June 18). *Kenya's financial services firms prime target for fraudsters*. Retrieved April 15, 2022, from East African: https://www.theeastafrican.co.ke/tea/business/kenya-identity-fraud-financial-services-industry-3441762

The Standard. (2022, February). *We must prioritize customer data security amid fintech growth*. Retrieved March 24, 2022, from Standard Media: https://www.standardmedia.co.ke/opinion/article/2001436121/we-must-prioritize-customer-data-security-amid-fintech-growth

Tiwari, A. (2019). *Security of Mobile Banking Application: Mobile Banking Technology.* Retrieved October 20, 2020, from http://www.suite101.com/content/security-of-mobile-banking-applicationmobile-banking-technology-a282550

Tobin, D. (2021, May 20). *What is Data Privacy and Why Is It Important?* Retrieved April 10, 2022, from Integrate: https://www.integrate.io/blog/what-is-data-privacy-why-is-it-important/

Tobin, P. (2011). Understanding Mobile Money Ecosystem: Roles, Structure and Strategies. Retrieved June 19, 2022, from https://www.semanticscholar.org/paper/Understanding-Mobile-Money-Ecosystem%3A-Roles%2C-and-Tobbin/47e5fa60d07c39ed6ab07cf0d0e5609d0ef01bf6

Truta, F. (2018, May 3). *59% of people use the same password everywhere, poll finds*. Retrieved April 24, 2021, from Security Boulevard: https://securityboulevard.com/2018/05/59-of-people-use-the-same-password-everywhere-poll-finds/

Tulkarm, P. (2021). A Survey of Social Engineering Attacks: Detection and Prevention Tools. *Journal of Theoretical and Applied Information Technology, 99*(18).

UK Finance. (2021). *Half Year Fraud Update.* Retrieved March 24, 2022, from https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

Union Bank. (2022). *Consumer Fraud Prevention and Awareness*. Retrieved March 24, 2022, from Union Bank Website: https://www.unionbank.com/privacy/consumer-fraud-education-and-awareness

van Teijlingen, R. E., & Hundley, V. (2001). *Social Research Update*. Retrieved April 30, 2020, from University of Surrey: http://sru.soc.surrey.ac.uk/SRU35.html

Vasileva, V. (2022). Application of a Human-Centric Approach in Security by Design for IoT Architecture Development. *International ISCIS Security Workshop* (pp. 13-22). Springer, Cham.

Verizon. (2023). *Data Breach Investigations Report.* Verizon. Retrieved July 18, 2025, from https://www.verizon.com/business/resources/reports/dbir/

Victor, D. (2014). On the User-centric Evolution of Mobile Money Technologies in Developing Nations: Successes and Lessons. *Twentieth Americas Conference on Information Systems.* Savannah.

Vodafone. (2022). *MPESA.* Retrieved April 24, 2022, from https://www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa

von Skarczinski, B. S., Dreissigacker, A., & Teuteberg, F. (2022). More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM.

Wang, C. X. (2021). CAFE: An instructional design model to assist K-12 teachers to teach remotely during and beyond the COVID-19 pandemic. *TechTrends, 65*(1), 8-16.

Wang, K., Guo, X., & Yang, D. (2022). Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics, 11*. Retrieved from https://doi.org/10.3390/electronics11101659

Wang, Q., Wang, D., Cheng, C., & He, D. (2021). Quantum2fa: efficient quantum-resistant two-factor authentication scheme for mobile devices. *IEEE Transactions on Dependable and Secure Computing*.

Wasson, B., & Kirschner, P. (2020). Learning design: European approaches. *TechTrends, 64*(6), 815-827. doi:https://doi.org/10.1007/s11528-020-00498-0

Wayne, S. (2022). Social Engineering: The Effects of Cybercriminals on the Human Mind. *Doctoral dissertation, Utica University*.

Weichbroth, P., & Łysik, L. (2020). Mobile Security: Threats and Best Practices. doi:https://doi.org/10.1155/2020/8828078

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security.* Cengage learning.

Whitney, L. (2021). *Awareness of cyberattacks and cybersecurity may be lacking among workers/ Armis Survey*. Retrieved March 16, 2022, from https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers

Windari, W., Batubara, S., & Sari, H. P. (2022). Strategy PT. Bank Sumut Syariah Panyabungan Branch Office In Improving The Quality Of Mobile Banking Services. *Islamic Financial Technology, 1*(1).

Wlosinski, L. (2019). The Benefits of Information Security and Privacy Awareness Training Programs. *Infromation Systems Audit and Control Association*.

Wood, C. (2021). Information Security Awareness Raising Methods. *Elsevier Science Ltd*.

Wood, C. C. (2019). *Information Security Policies Made Easy, Version 7.* San Deigo: PentaSafe Security Technologies, Inc.

World Bank. (2020). *Cybersecurity in financial sector development: Challenges and potential solutions.* Retrieved 2025, from worldbank.org: https://documents1.worldbank.org/curated/en/209721593689624542/pdf/Cyber-Security-in-Financial-Sector-Development-Challenges-and-Potential-Solutions-for-Financial-Inclusion.pdf

Yeboah, T. (2016). A Proposed Information Technology Audit Framework for Microfinance Kumasi.

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management, 19*.

Yulianti, T., & Sulistiyawati, A. (2020). The Blended Learning for Student's Character Building. *In International Conference on Progressive Education (ICOPE 2019)* (pp. 56-60). Atlantis Press.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of applied security research*, *16*(4), 490-513.

Zeisl, Y. (2019, November 26). *Fintech Growth in Kenya: The Success of Mobile Money*. Retrieved April 24, 2021, from Global Rist Intel: https://www.globalriskintel.com/insights/fintech-growth-kenya-success-mobile-money

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97.

Annexures

ANNEXURE A:

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

17 July 2013

Safaricom Limited
Safaricom House
Waiyaki Way
P.O. Box 66827-00100
NAIROBI

Dear Sirs

RE: INDEMNITY IN RESPECT OF THE RESEARCH TO BE UNDERTAKEN BY NICHOLAS WASHINGTON OMOLLO AT SAFARICOM LIMITED

We refer to the above matter.

We write to confirm that Nicholas Washington Omollo is a PHD student based at the University of KwaZulu Natal. In fulfillment of the requirements for his PHD project, he will be focusing on the Information Security Education, Training and Awareness within the Mobile Financial Services.

Nicholas W. Omollo has by an email dated February 6th 2013 requested to be allowed to undertake his research at Safaricom Limited. We are aware that in the course of his research he may receive Confidential Information utilized in the course of Safaricom's business operations.

In this regard the Univeristy of KwaZulu Natal hereby agrees to indemnify and hold harmless Safaricom Limited from and against all claims, liabilities, losses, damages, and expenses incurred (including any legal costs or penalties and liabilities awarded or imposed by a court or expenses properly incurred) by Nicholas W. Omollo pursuant to any breach or non-observance by his obligations or warranties under the Non-Disclosure Agreement which he has executed with Safaricom Limited.

For and on behalf of the University of KwaZulu-Natal

[redacted]

Professor Manoj S Maharaj
Thesis Supervisor

Manoj Maharaj

Digitally signed by Manoj Maharaj
DN: cn=Manoj Maharaj, o=University of KwaZulu-Natal, ou=Management, IT and Governance, email=maharajms@ukzn.ac.za, c=ZA
Date: 2013.07.17 18:43:55 +02'00'

School of Management, IT & Governance- Research & Higher Degrees
Postal Address: Room 237, 2nd Floor, M Block, Westville Campus, Westville, 3630
Telephone: +27 (0) 31 260 8162 Pearcea2@ukzn.ac.za **Website:**www.ukzn.ac.za

ANNEXURE B: UKZN PERMISSION TO CONDUCT RESEARCH I

UNIVERSITY OF KWAZULU-NATAL

February 16, 2013

To Whom It May Concern:

PERMISSION TO CONDUCT RESEARCH AS PART OF THE PhD QUALIFICATION

Name: NICHOLAS WASHINGTON OMOLLO

Student No: 212559707

Dissertation Topic: Information Security Education, Training and Awareness within the Mobile Financial Services Sector

It is a requirement of our PhD qualification that all students undertake intensive, high-level research. Typically this research necessitates data gathering through questionnaires or interviews.

Your assistance in permitting access to your organization for purposes of this research is most appreciated. The research will also involve some of your clientele using mobile devices for financial service solutions. Please be assured that all information gained from the research will be treated confidentially. This is a significant requirement of the University's internal ethical clearance requirements. All data presented in the final document will be di-identified. The student will strictly adhere to any additional confidentiality and anonymity requirements that you may require.

If permission is granted the University of KwaZulu-Natal requires this to be in writing on a letterhead and signed by the relevant authority.

Thank you for your assistance in this regard.

Yours sincerely

[redacted]

Professor M S Maharaj (Thesis Supervisor)

Office M1-5
Westville Campus
UKZN
maharajms@ukzn.ac.za

031 260 8023
031 260 7051
[redacted]

ANNEXURE C: UKZN PERMISSION TO CONDUCT RESEARCH II

UNIVERSITY OF KWAZULU-NATAL

14th May 2020

To Whom It May Concern:

PERMISSION TO CONDUCT RESEARCH AS PART OF THE PhD QUALIFICATION

Name: NICHOLAS WASHINGTON OMOLLO

Student No: 212559707

Dissertation Topic: Information Security Education, Training and Awareness within the Mobile Financial Services Sector

It is a requirement of our PhD qualification that all students undertake intensive, high-level research. Typically, this research necessitates data gathering through questionnaires or interviews.

Washington's research will be conducted in 6 major towns in Kenya.

This study process is expected to take 3 months beginning September 1st 2020.

This letter is to formally request you to grant him permission to proceed to the field to gather the needed data.

Thank you for your assistance in this regard.

Yours sincerely

[redacted]

Professor M S Maharaj (Thesis Supervisor)

Office M1-5
Westville Campus
UKZN
maharajms@ukzn.ac.za

031 260 8023
031 260 7051
[redacted]

ANNEXURE D: PERMISSION TO CONDUCT RESEARCH: GATEKEEPER'S LETTER I

Communications Commission of Kenya

Our Ref: CCK/CTMA/Research/Vol.13/10/05

10th May, 2013

Professor M. S. Maharaj (Thesis Supervisor)
University of Kwazulu-Natal
Office M1-5
Westville Campus
UKZN.

Dear Prof Maharaj

RE: PERMISSION TO CONDUCT RESEARCH AS PART OF THE PHD QUALIFICATION – NICHOLAS WASHINGTON OMOLLO

Your letter on the above subject refers.

We are in receipt of your letter requesting the Commission to permit access to our organization for purposes of this research to be carried out by Nicholas Washington Omollo.

The Commission has not objection to allowing the aforementioned student to carry out the interview at the Commission.

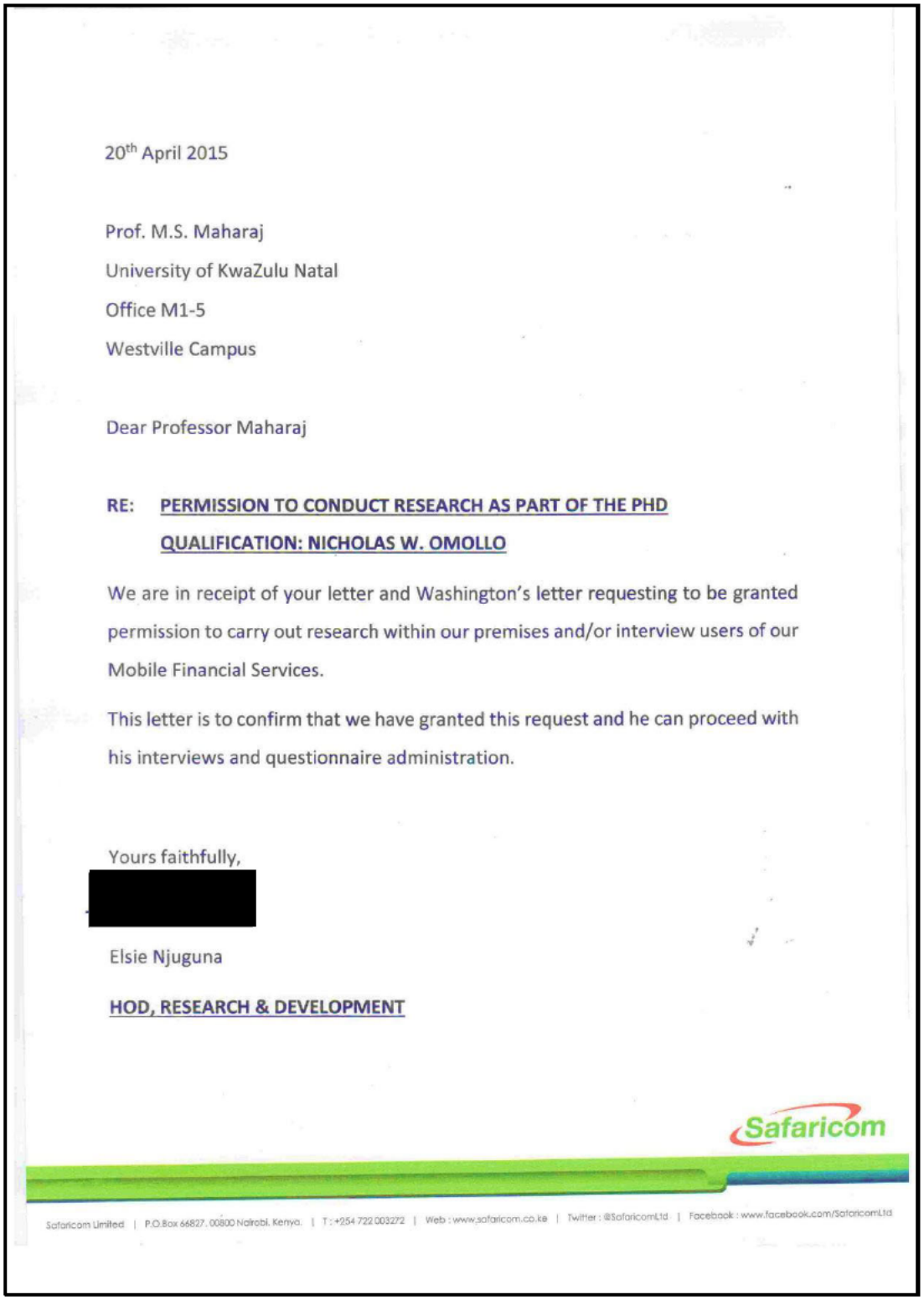
Yours faithfully,

[redacted]

Matano m. Ndaro
FOR: DIRECTOR-GENERAL

CCK Centre, Waiyaki Way, P.O. BOX 14448 Nairobi 00800, Kenya
Telephone: +254 20 4242000 Fax: 254 20 4451866 / 4242207 / 4348204

ANNEXURE E: PERMISSION TO CONDUCT RESEARCH: GATEKEEPER'S LETTER II



20th April 2015

Prof. M.S. Maharaj
University of KwaZulu Natal
Office M1-5
Westville Campus

Dear Professor Maharaj

RE: PERMISSION TO CONDUCT RESEARCH AS PART OF THE PHD QUALIFICATION: NICHOLAS W. OMOLLO

We are in receipt of your letter and Washington's letter requesting to be granted permission to carry out research within our premises and/or interview users of our Mobile Financial Services.

This letter is to confirm that we have granted this request and he can proceed with his interviews and questionnaire administration.

Yours faithfully,

[redacted]

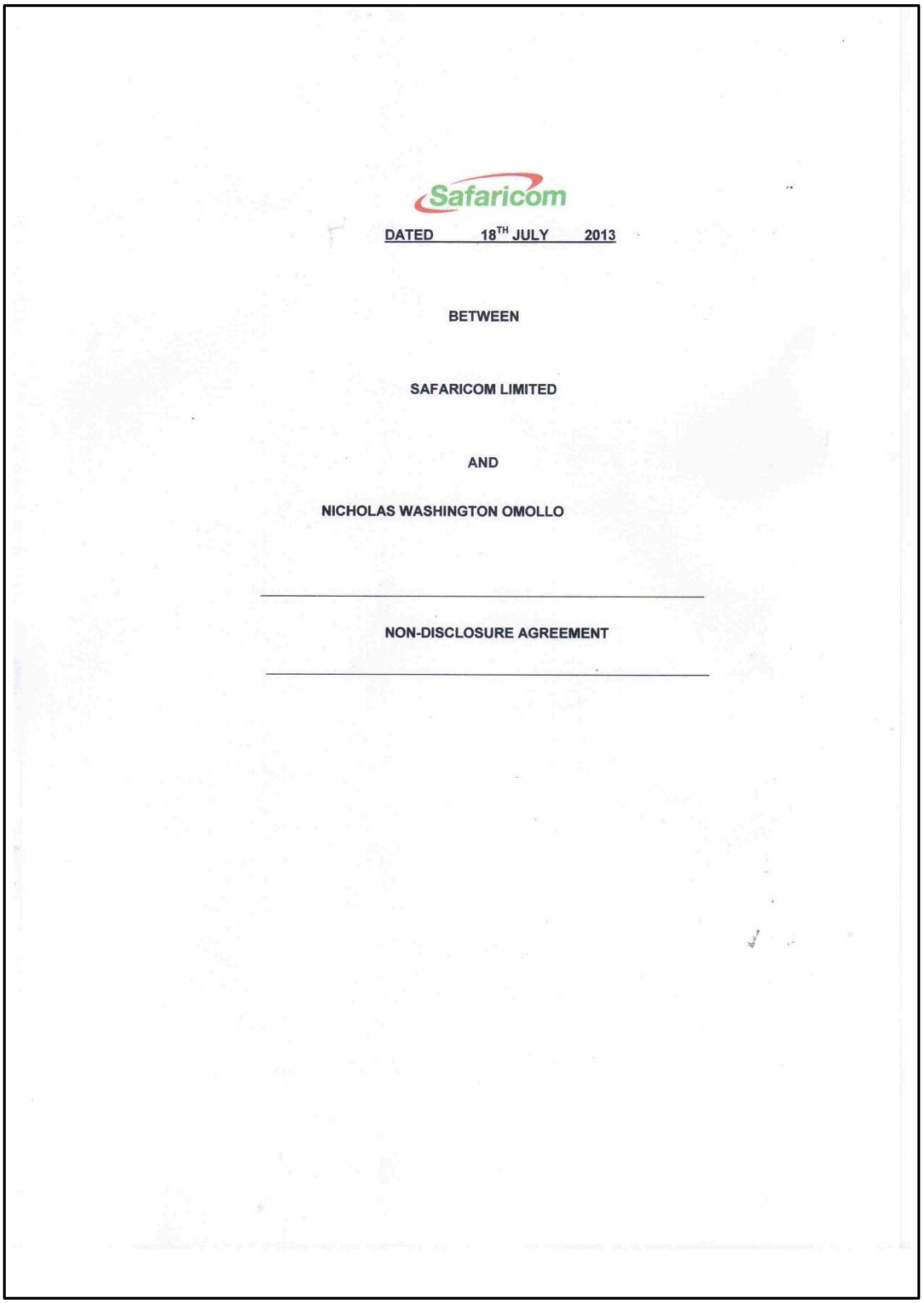
Elsie Njuguna

HOD, RESEARCH & DEVELOPMENT

Safaricom

Safaricom Limited | P.O.Box 66827, 00800 Nairobi, Kenya. | T: +254 722 003272 | Web: www.safaricom.co.ke | Twitter: @SafaricomLtd | Facebook: www.facebook.com/SafaricomLtd

ANNEXURE F: PERMISSION TO CONDUCT RESEARCH: NON-DISCLOSURE AGREEMENT



Safaricom

DATED 18TH JULY 2013

BETWEEN

SAFARICOM LIMITED

AND

NICHOLAS WASHINGTON OMOLLO

NON-DISCLOSURE AGREEMENT

TABLE OF CONTENTS

THIS NON-DISCLOSURE AGREEMENT (this "**Agreement**") is made the.....18th.....day of .....July..... **2013 ("the Effective Date") BETWEEN**:

1 **SAFARICOM LIMITED** a limited liability company incorporated in the Republic of Kenya and having its principal office at Safaricom House, Waiyaki Way, Nairobi and of P.O. Box 66827-00800, Nairobi, Kenya (**"Safaricom"**) of the one part; and

2 **NICHOLAS WASHINGTON OMOLLO** whose registered physical location is care of the SDA Church, East Africa Union, Milimani Road ("hereinafter called **"the Student"**) of the other part.

(Each of which may be referred to as a "**Party**" and collectively as the "**Parties**")

WHEREAS

A. Safaricom is about to release certain information pertaining to Information Security Education, Training and Awareness within the Mobile Financial Services to facilitate a PHD project on understanding the issues and challenges surrounding security of transactions in mobile financial services, Understand mobile security as a concept and mobile security as a challenge to users and service providers and investigate the state of mobile Security, Education Training, and Awareness for users and professionals. (the "Purpose")

B. This Agreement is being executed in connection with the disclosure of information that will be undertaken for the Purpose set out in (A) above.

C. Safaricom has agreed to disclose the information on condition that the acknowledges he will gain access to Proprietary Information (as defined in Clause 1.3) of Safaricom and is legally bound by the terms of this Agreement, and shall maintain the confidentiality of all such Proprietary Information in accordance with this Agreement.

NOW THEREFORE, in consideration of the mutual promises and covenants made herein and for other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties, each intending to be legally bound, agree as follows:

1 DEFINITIONS

1.1. "**Disclosing Party**" means Safaricom Limited or any of its Parent or Subsidiary companies.

1.2. "**Receiving Party**" means the Student.

1.3. "**Confidential Information**" means all information and know-how, regardless of whether or not in writing, of a private, secret or confidential nature that relates to the business, technical or financial affairs of the Disclosing Party, its subsidiaries, affiliates, customers, potential customers, suppliers or potential suppliers, provided or disclosed to the Receiving Party or which becomes known to the Receiving Party, whether or not marked or otherwise designated as "confidential", "Confidential" or with any other legend indicating its Confidential nature. Confidential Information includes, by way of illustration and not limitation, all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, inventions and developments, products, formulas, designs, prototypes, methods, techniques, processes, procedures, computer programs and software (whether as source code or object code), documentation, technologies, plans,

the Supplier's information, customer information, personnel information, research, and reports, whether tangible or intangible, and whether or not stored, compiled, or memorialised physically, electronically, graphically, photographically, or in writing. Confidential Information shall further include any such information, materials, tangible or intangible property of customers of, suppliers to or any other third party with whom the Disclosing Party does or considers doing business and who may have disclosed or entrusted such information to a Receiving Party pursuant to or in furtherance of the discussions and exchanges under this Agreement.

1.4. Confidential Information shall **not** include information that:

1.4.1. has become public knowledge through legal means without fault by the Receiving Party,

1.4.2. is already public knowledge prior to the Disclosing Party's disclosure of the same to the Receiving Party,

1.4.3. is known to the Receiving Party prior to the Disclosing Party's disclosure of the same pursuant to this Agreement, or

1.4.4. is independently developed by the Receiving Party without reference to or use of the Confidential Information.

2 DUTIES

With respect to the Disclosing Party's Confidential Information, the Receiving Party agrees that he shall secure and keep such Confidential Information and:

1.5. not disclose it, or allow it to be disclosed in whole or in party to any third party without the consent of Safaricom;

1.6. keep it in a safe and secure place and use reasonable measures to prevent unauthorized access, destruction, corruption or loss;

1.7. not make any copies, summaries or transcripts of it unless this is strictly necessary for the Purpose (all such copies, summaries or transcripts will be deemed to be Confidential information;

1.8. not export it or permit it to be exported in breach of any relevant export regulation;

1.9. notify the Disclosing Party immediately he becomes aware that any Confidential Information has been disclosed to, or is in the possession of any person or company undertaking any business in competition with the Disclosing Party;

1.10. Notwithstanding the foregoing, the Receiving Party shall be entitled to release Confidential Information to permit it to prosecute or defend any claim under this Agreement or pursuant to an order of a court or government agency; provided, however, in the case of release pursuant to this clause, the Receiving Party shall limit the release to the greatest extent reasonably possible under the circumstances and shall have provided the Disclosing Party with sufficient advance notice to permit the Disclosing Party to seek a protective order or other order protecting its Confidential Information from disclosure.

3 OWNERSHIP

All Confidential Information, including that which is contained in files, letters, memoranda, reports, records, data, sketches, drawings, notebooks, program listings, or other written, photographic, or other tangible, intangible, or other materials, or which shall come into a Receiving Party's custody or possession, is and at all times shall be the exclusive property of the Disclosing Party, to be used by the Receiving Party only for the purposes expressly contemplated by this Agreement.

4 NO RIGHTS OR LICENSES GRANTED

The Receiving Party shall not acquire hereunder any right whatsoever to any Confidential Information, including without limitation any right or license of any patent, trademark, copyright, trade secret, moral right or any other right now or later recognized by any law or regulation of any jurisdiction throughout the universe (collectively, "**Intellectual Property Rights**") as a result of or in connection with any disclosure hereunder. Accordingly, nothing in this Agreement is intended or shall be construed as a transfer, grant, license, release or waiver of any Intellectual Property Rights in any Confidential Information.

5 RETURN OF CONFIDENTIAL INFORMATION

At the request of the Disclosing Party or upon termination of this Agreement, the Receiving Party shall promptly destroy all of its copies of such Confidential Information or return the same to Disclosing Party and make no further use or disclosure of it and in either case shall, within fourteen (14) days of receiving such a request, obtain a certification in writing of his compliance with the terms of this provision. After such destruction or delivery, the Receiving Party shall not retain any copies thereof.

6 NO OBLIGATION

Nothing in this Agreement shall be deemed to obligate the Disclosing Party to disclose any Confidential Information to the Receiving Party.

7 REMEDY

The Receiving Party acknowledges the insufficiency of monetary damages as a remedy for any breach of this Agreement by a Receiving Party, and that any such breach could cause the Disclosing Party irreparable harm. Accordingly, the Disclosing Party, as the case may be, in addition to any other remedies available at law, shall be entitled to specific performance and injunctive or other equitable relief as a remedy for any such breach. If litigation arises relating to this Agreement, and a court of competent jurisdiction determines that the Receiving Party, has breached this Agreement, the Receiving Party shall be liable and shall pay to the Disclosing Party the reasonable legal fees incurred by the prevailing Party in connection with such litigation, including any appeals therefrom.

8 SEVERABILITY

The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement.

9 NO WAIVER

No delay or omission by the Disclosing Party in exercising any right under this Agreement will operate as a waiver of that or any other right. A waiver or consent given by the Disclosing Party on any occasion is effective only in that instance and will not be construed as a bar to or waiver of any right on any other occasion.

10 GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws of Kenya.

11 ARBITRATION

11.1 Any dispute arising out of or in connection with this Agreement shall be referred to arbitration by a single arbitrator to be appointed by agreement between the parties or in default of such agreement within fourteen (14) days of the notification of a dispute, upon the application of either party, the

arbitrator shall be appointed by the Chairman for the time being of the Kenya Branch of the Chartered Institute of Arbitrators of the United Kingdom.

11.2 Such arbitration shall be conducted in Nairobi in accordance with the Rules of Arbitration of the said Institute and subject to and in accordance with the provisions of the Arbitration Act 1995.

11.3 To the extent permissible by law, the determination of the Arbitrator shall be final conclusive and binding upon the parties.

11.4 Pending final settlement or determination of a dispute, the parties shall continue to perform their subsisting obligations hereunder.

11.5 Nothing in this Agreement shall prevent or delay a party seeking urgent injunctive or interlocutory relief in a court having jurisdiction.

12 NO RELATIONSHIP CREATED

Nothing in this Agreement shall be construed as establishing or implying any partnership, or agency between the Parties, or authorize the Receiving Party to commit or bind the Disclosing Party in any way whatsoever without obtaining the Disclosing Party's prior written consent.

13 TERM

The disclosure under this Agreement shall commence on the Effective Date and shall continue for a period of two (2 years unless sooner terminated upon prior written notice of at least one (1) month by one Party to the other. The obligations of confidentiality on the Receiving Party under this Agreement with respect to all Confidential Information shall survive the termination or expiration of this Agreement.

14 AMENDMENTS IN WRITING

No amendment or modification of any term of this Agreement shall be valid or binding on the Parties unless made in writing and executed on behalf of each Party by a duly authorized representative.

15 NO WARRANTY

No disclosure of any Confidential Information by the Disclosing Party shall constitute any representation or warranty by the Disclosing Party regarding the accuracy of the same or the non-infringement of any patent, trademark, copyright or any other intellectual property or Confidential right.

16 NO PUBLICATION

The Receiving Party shall not publicize or advertise in any manner the Confidential information contemplated by the Agreement without the prior written consent of the Disclosing Party, except as may be required by law.

17 ENTIRE AGREEMENT

This Agreement constitutes the entire agreement between the Parties hereto concerning the subject matter hereof and supersedes any prior or contemporaneous agreements and understandings concerning the subject matter hereof.

18 COUNTERPARTS

This Agreement and any amendment hereto may be executed in counterparts, each of which when executed and delivered shall be deemed an original and all of which taken together shall constitute one and the same instrument. This Agreement may be delivered by facsimile.

19 NOTICES

19.1 All notices, requests and consents under this Agreement shall be in writing and shall be deemed to have delivered (a) on the date personally delivered, (b) on the date mailed, postage prepaid by certified mail with return receipt requested.

19.2 The Parties select as their respective addresses, the addresses set out below for all purposes arising out of or in connection with this Agreement at which addresses only all processes and notices arising out of or in connection with this Agreement may validly be served upon or delivered by the Parties.

SAFARICOM:
The Chief Executive Officer
Safaricom Limited
Safaricom House
Waiyaki Way, Westlands
P.O. Box 66827-00800
Nairobi, Kenya.

THE STUDENT:
Nicholas Washington Omollo
c/o SDA Church, East Africa Union
Milimani Road
P.O. Box 42276, 00100
Nairobi, Kenya

20 HEADINGS

Headings used in this Agreement are for reference only and shall not affect the interpretation of this Agreement in any way.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the Effective Date and agree to be legally bound by all terms and conditions contained herein.

SIGNED BY:
Duly authorised for and on behalf of:
SAFARICOM LIMITED
in the presence of:

.....
(Signature)

SIGNED BY:
Mr. Nicholas Washington Omollo
.....
(Name & Title)

[redacted]
.....
(Signature)

In the presence of:

[redacted]REDRICK OTIENO MEGB
ADVOCATE
[redacted] P. O. Box 61901 - 00200 NAIROBI

ANNEXURE G: RESEARCH INSTRUMENT I: QUESTIONNAIRE FOR MFS PROVIDERS

UNIVERSITY OF KWAZULU-NATAL
SCHOOL OF MANAGEMENT, IT & GOVERNANCE
PhD Research Project

Researcher: Nicholas Washington Omollo (+[redacted])
Supervisor: PROF. Manoj Maharaj (+27 31 260 7051)
Research Office: Ms. M Snyman (+27 31 260 8350)

Dear Respondent,

I, Nicholas Washington Omollo, am a PhD student at the School of Management, IT and Governance, University of KwaZulu-Natal, Durban, South Africa. You are invited to participate in a research project entitled "Information Security Education, Training and Awareness within the Mobile Financial Services Sector." The aim of this study is to: develop a baseline framework body of knowledge for information Security Awareness, Education and Training for end users and professionals within the Mobile Financial Services sector to help improve security in the operations and reduce risks associated with end users.

Through your participation I will identify the issues and challenges surrounding security of transactions in mobile financial services, understand mobile security as a concept and mobile security as a challenge to users and service providers and investigate the state of mobile Security, Education Training, and Awareness for users and professionals.

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Management, IT and Governance, University of KwaZulu-Natal.

1

If you have any questions or concerns about participating in this study, please contact me or my supervisor at the numbers listed above.

I hope you will take a few minutes to complete the questionnaire.

Sincerely,

Nicholas Washington Omollo

CONSENT

I, ……hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project.

I understand that I am at liberty to withdraw from the project at any time, should I so desire.

…… ……

SIGNATURE OF PARTICIPANT DATE

1. Which sector do you work in?

   (a) Bank [ ]
   (b) Telecom provider [ ]
   (c) Finance regulator [ ]
   (d) Telecommunications regulator [ ]

2. Does your organisation have a Mobile Money security awareness programme for end users?

   (a) Yes [ ]
   (b) No [ ]

3. If YES is 2 above, how often does your organisation run the security awareness programme for end users?

   (a) Monthly [ ]
   (b) Quarterly [ ]
   (c) Half yearly [ ]
   (d) Yearly [ ]
   (e) Randomly [ ]

4. To what extent do you agree with the following statements?

Key Areas	Strongly Disagree	Disagree	Uncertain	Agree	Strongly Agree
Our customers have been adequately trained on how to ensure security when conducting financial transactions on their mobile devices.					
We have adequately trained our customers on how to physically secure their mobile devices.					
Our Mobile financial security awareness programme takes into consideration the age of end users.					

Our Mobile financial security awareness programme takes into consideration the education of end users.					

5. Please rank (by ticking the box) the following Mobile Financial Security Awareness delivery methods in order of your organisation's preference. (1- Least Preferred to 5- Most Preferred)

Training Delivery Method	Preference Scale (Rank)				
	1	2	3	4	5
Posters					
Periodic SMS alerts.					
Person-to-Person interaction.					
Television adverts.					
Radio announcement in local dialects.					
Road shows and other open field activities.					
Periodic newsletter.					
Newspaper advertisements.					
Classroom workshops.					
E-Mail.					
Web based training.					
Online discussion.					
Short video-based methods.					

6. The table below lists a number of common mobile users' security concerns. To what extent are the issues a concern to your organisation. Please rank in a scale of 1-5 where 1 is of least concern and 5 of most concern.

Security Threats	Priority Scale (Rank)				
	1	2	3	4	5
Loss of mobile devices.					

Users storing personal information on mobile device.					
Users installing rogue applications and malware on their mobile phones.					
User sharing Mobile Banking PINs/Passwords.					
Users installing malicious software on their mobile devices.					
Social engineering attacks.					
Mobile devices and applications vulnerabilities.					

7. To what extent are the following security concerns included in your organisation's awareness programmes? Please rank in a scale of 1-5 where 1-Least included and 5-Always included.

Information Security Concept	**Priority Scale (Rank)**				
	1	**2**	**3**	**4**	**5**
Physical Protection of Mobile Devices.					
Vulnerabilities/Password confidentiality.					
Social Engineering.					
MFS Fraud incident early detection.					
Strong Security Password setup.					
Mobile Money Risks (theft of phone, Money sent to wrong number, PIN leakage to another person, fake money from agent, fake transaction detections.					

8. To what extent do you agree with the following statements on the Mobile Financial Service regulatory framework in Kenya?

Key Areas	**Strongly Disagree**	**Disagree**	**Uncertain**	**Agree**	**Strongly Agree**
Law adequately protects the consumer.					
Law affects the stability of banking/national payment system.					

Law adequately distinguishes between deposits and payments.					
Law provides for e-Money issuance.					
Law provides for agencies for cash withdrawals and deposits – i.e., authority to deposit or withdraw cash by agents.					
Law adequately covers Anti-Money Laundering (AML).					

ANNEXURE H: RESEARCH INSTRUMENT II: QUESTIONNAIRE FOR MFS SUBSCRIBERS

UNIVERSITY OF KWAZULU-NATAL
SCHOOL OF MANAGEMENT, IT & GOVERNANCE

PhD Research Project

Researcher: Nicholas Washington Omollo (+2[redacted])
Supervisor: PROF. Manoj Maharaj (+27 31 260 7051)
Research Office: Ms. M Snyman (+27 31 260 8350)

Dear Respondent,

I, Nicholas Washington Omollo am a PhD student, at the School of Management, IT and Governance, University of KwaZulu-Natal, Durban. You are invited to participate in a research project entitled "Information Security Education, Training and Awareness within the Mobile Financial Services Sector". The aim of this study is to: develop a baseline framework body of knowledge for information Security Awareness, Education and Training for end users and professionals within the Mobile Financial Services sector to help improve security in the operations and reduce risks associated with end users.

Through your participation I will identify the issues and challenges surrounding security of transactions in mobile financial services, understand mobile security as a concept and mobile security as a challenge to users and service providers and investigate the state of mobile Security, Education Training, and Awareness for users and professionals.

Your participation in this project is voluntary. You may refuse to participate or withdraw from the project at any time with no negative consequence. There will be no monetary gain from participating in this survey. Confidentiality and anonymity of records identifying you as a participant will be maintained by the School of Management, IT and Governance, University of KwaZulu-Natal.

1

If you have any questions or concerns about participating in this study, please contact me or my supervisor at the numbers listed above.

I hope you will take a few minutes to complete the questionnaire.

Sincerely

[redacted]

Nicholas Washington Omollo

CONSENT

I, ……hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project.

I understand that I am at liberty to withdraw from the project at any time, should I so desire.

…… ……

SIGNATURE OF PARTICIPANT DATE

SECTION A: DEMOGRAPHIC INFORMATION

1. Gender

   (a) Male [ ]
   (b) Female [ ]

2. Age

   (a) 18-25 years [ ]
   (b) 25-40 years [ ]
   (c) 41-50 years [ ]
   (d) 51-60 years [ ]
   (e) 61years and above [ ]

3. What is your highest level of Education

   (a) No formal education [ ]
   (b) KCPE Certificate [ ]
   (c) KCSE Certificate [ ]
   (d) Artisan /Craft Certificate [ ]
   (e) Diploma [ ]
   (f) Bachelor's Degree [ ]
   (g) Master's Degree [ ]
   (h) PhD [ ]

4. How can you best describe your main place of residence?

   (a) Big City [ ]
   (b) Big Town [ ]
   (c) Small Town [ ]
   (d) Rural Area [ ]

SECTION B: ASSESSING THE CONCEPTS ON INFORMATION SECURITY

1. For how long have you owned a mobile phone?

   (a) 0-5 years [ ]
   (b) 6-10 years [ ]
   (c) 11-15 years [ ]
   (d) 16 years and above [ ]

2. Who is your service provider? You can select more than one if applicable.

   (a) Safaricom [ ]
   (b) Airtel [ ]
   (c) Yu [ ]
   (d) Orange [ ]

(e) Equitel [ ]

3. Which of the following services do you access on your phone? (Tick all that apply)

(a) MPESA/Airtel Money/T-Cash [ ]
(b) M-Banking (Getting your banks services on your phone) [ ]
(c) SMS [ ]
(d) Voice [ ]

4. To what extent do you trust the mobile platform when undertaking a financial transaction.

Very Small Extent	Small Extent	Never	Large Extent	Very Large Extent

5. How often do you seek assistance from people with your phone to carry out MPESA/Mobile Money transaction?

(a) Always [ ]
(b) Many times [ ]
(c) Once [ ]
(d) Never [ ]

6. On a scale of 1 to 5 (1-Least confident, 5-Most confident), how would you rate your confidence when using your phone to perform MPESA/Mobile money transaction without requiring help from someone else?

1		2		3		4			5	

7. To what extent do you feel money kept in your mobile wallet is safe from theft/loss?

Very Small Extent	Small Extent	Never	Large Extent	Very Large Extent

8. Are you aware that your phone has settings that allows you to auto-lock your phone when it is not in use for some time?

(a) Yes [ ]
(b) No [ ]

9. Are you aware that you can set a password that is not easy to guess for your phone or mobile money (for example not using date of birth or repeating digits in your password)?

   (a) Yes [ ]
   (b) No [ ]

10. Do you know how to physically secure your phone i.e., put auto lock password and require password to unlock without help?

    (a) Yes [ ]
    (b) No [ ]

11. Does your mobile phone have any password/security code for locking?

    (a) Yes [ ]
    (b) No [ ]
    (c) I don't know [ ]

12. Are you aware you should not use the same security code/password for mobile money to access your other social networks e.g., E-Mail, Facebook, Twitter accounts, google etc.?

    (a) Yes [ ]
    (b) No [ ]

13. Are you aware you can change your MPESA PIN/ password after sometime or as often as you may want?

    (a) Yes [ ]
    (b) No [ ]

14. Have you shared your mobile money PIN/Password with others to perform a transaction?

    (a) Yes [ ]
    (b) No [ ]

15. Have you shared your phone with someone to help you with a transaction?

    (a) Yes [ ]
    (b) No [ ]

16. Have you shared your government registration ID card/Passport to someone to withdraw MPESA for you?

(a) Yes [ ]
(b) No [ ]

17. To what extent are you concerned that someone can use your ID and do a SIM Swap and use it to commit fraud?

Very Small Extent	Small Extent	Never	Large Extent	Very Large Extent

18. Are you aware that you are not supposed to keep your MPESA PIN/Mobile bank password as a draft message on your phone?

(a) Yes [ ]
(b) No [ ]

19. Have you set your phone to show password/PIN when entering it (so you can easily know what you typed)?

(a) Yes [ ]
(b) No [ ]

20. To what extent are you concerned that when you share/or when someone gets to know your password/PIN, they can use it later to commit fraud/remove money from your account/mobile wallet without you knowing?

Very Small Extent	Small Extent	Never	Large Extent	Very Large Extent

21. To what extent do you think you can recognise if your phone has been hacked?

Never	Rarely	Sometimes	Most of the Time	Always

22. Have you ever lost money through a Mobile Money Transaction?

(a) Yes [ ]
(b) No [ ]

23. If so, what caused you to lose money (Tick all that apply)?

Fictitious Transaction Request	Tick ( )
I lost the phone. Somebody then used my phone to transact without my knowledge.	
I gave the phone/PIN to someone I trust then they used the phone to commit the fraud.	
Someone stole my password and used it to commit fraud.	
I accidentally sent money to a wrong number.	
I do not know how.	

24. How did you report if you have lost money via MPESA/Mobile Banking?

(a) Police [ ]
(b) Service Provider [ ]
(c) I just keep quiet [ ]
(d) Any other (Specify)

25. Have you ever attended an awareness session on mobile security?

(a) Yes [ ]
(b) No [ ]

26. If **YES** in 25 above, to what extent did you like the awareness session (i.e., was the awareness helpful to you)?

(a) Yes [ ]
(b) No [ ]

27. If **NO** in 26 above, what did you not like in the awareness session? Tick ALL that apply.

(a) Content was not appropriate [ ]
(b) Mode of training was not appropriate [ ]
(c) It was not interesting [ ]
(d) Any other (Please specify) [ ]

28. Which of the following is your most preferred awareness delivery method? (Tick your best 3).

(a) Posters [ ]

(b) Periodic SMS blasts [ ]
(c) Person to Person Interaction [ ]
(d) TV adverts [ ]
(e) Radio announcements in my local dialects [ ]
(f) Local skits [ ]
(g) Road Shows in our local area [ ]
(h) Newsletter [ ]
(i) Newspaper ads [ ]
(j) Classroom workshops [ ]
(k) E-mail [ ]
(l) Web-based training [ ]
(m)Online Discussion [ ]
(n) Video-based methods [ ]

29. Do you keep Personally Identifiable Information (e.g., your name, bank account number etc) on your phone?

(a) Yes [ ]
(b) No [ ]

30. Do you use your phone to access the internet i.e., Facebook, Twitter, Yahoo mail, google etc.?

(a) Yes [ ]
(b) No [ ]

31. Do you enable location services on your phone?

(a) Yes [ ]
(b) No [ ]
(c) I don't know [ ]

32. Have you ever downloaded applications and documents from the internet intentionally or unknowingly?

(a) Yes [ ]
(b) No [ ]

33. To what extent do you trust the safety of websites you normally access through your phone?

Unsafe Most of the Time	Sometimes Unsafe	Generally Safe	Safe Most of the Time	Safe All of the Time

34. Does your phone have an anti-virus program?

(a) Yes [ ]
(b) No [ ]
(c) I don't know [ ]

35. To what extent are you concerned that some files you download might collect some data from your phone without your knowledge?

Very Small Extent	Small Extent	Never	Large Extent	Very Large Extent

36. Are you aware of any security risks associated with using mobile devices?

(a) Yes [ ]
(b) No [ ]

37. Are you aware you can disable location settings on your phone

(a) Yes [ ]
(b) No [ ]

38. Do you know how to change settings/location services on your phone?

(a) Yes [ ]
(b) No [ ]

39. Do you think information/data in your phone is important?

(a) Yes [ ]
(b) No [ ]

40. Have you ever heard of mobile security?

(a) Yes [ ]
(b) No [ ]

41. Do you know your roles and responsibility in ensuring secure mobile financial service?

(a) Yes [ ]
(b) No [ ]

42. Do you have an idea of any "social engineering" tricks for mobile devices or what it means?

(a) Yes [ ]
(b) No [ ]

43. To what extent do you think you can identify a mobile money hoax (scam) i.e., someone asking you to pay some money to get a prize or someone posing as friend and that they are stuck and needs some money.

Very Small Extent	Small Extent	Never	Large Extent	Very Large Extent

44. Have you encountered a phishing attack is (i.e., someone asking for your MPESA PIN, National ID etc)?

(a) Yes [ ]
(b) No [ ]

45. Have you had/experienced a phishing attack i.e., someone asking you to call them to claim some money that you have won or someone sending you a message with instructions on how to claim some money you have won?

(a) Yes [ ]
(b) No [ ]

46. If **YES** in 45 above, how did you respond?

(a) I did as they requested [ ]
(b) I reported to the police [ ]
(c) Did nothing [ ]

47. Do you think Mobile Money security awareness is a challenge that needs to be addressed?

(a) Yes [ ]
(b) No [ ]

48. Are you aware of any laws governing mobile security in Kenya?

(a) Yes [ ]
(b) No [ ]

49. Do you think there is a need to have a mobile Security Education Training and Awareness in Kenya?

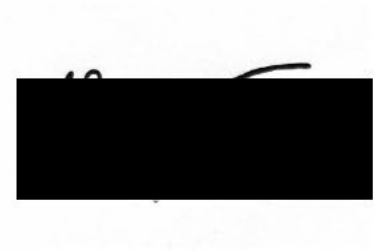
(a) Yes [ ]
(b) No [ ]

50. If **YES** in 49 above, on a scale of 1-5, (1-Least priority, 5-High priority), how would you want the following information security concepts be considered for training and awareness?

Information Security Concept	Priority Scale				
	1	2	3	4	5
Physical Protection of Mobile Devices.					
Vulnerabilities/Password confidentiality.					
Emerging threat and detection (Phishing and vishing schemes).					
MFS Fraud incident early detection.					
Damage/Loss caused by use of Mobile Money use, Failure, malfunction, interruption or unavailability of the Mobile Financial System.					
Strong Security Password setup.					
Mobile Money Risks (theft of phone, Money sent to wrong number, PIN leakage to another person, fake money from agent, fake transaction detections.					
Any other (Please Specify).					

ANNEXURE I: LANGUAGE EDITING CERTIFICATE

We the undersigned, do solemnly declare that we have abided by the University of KwaZulu-Natal's policy on language editing. The thesis was professionally edited for proper English language, grammar, punctuation, spelling, and overall academic style. All original electronic forms of the text have been retained should they be required.



GARY STUART DAVID LEONARD

UKZN Higher Degrees Certified Language Editor

Commissioner of Oaths V3358

NICHOLAS WASHINGTON OMOLLO

ANNEXURE J: RESEARCH PROTOCOL RECERTIFICATION

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

6 September 2019

Mr Nicholas Washington Omollo (212559707)
School of Management, IT and Governance
Westville Campus

Dear Mr Omollo,

Protocol reference number: HSS/1508/015D
Project title: Information Security Education, Training and Awareness within the Mobile Finacial Services Sector

Approval Notification - Recertification Application

Your request for Recertification dated 28 August 2019 was received.

This letter confirms that you have been granted Recertification Approval for a period of one year from the date of this letter. This approval is based strictly on the research protocol submitted and approved in 2015.

Any alteration s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study must be reviewed and approved through the amendment
/modification prior to its implementation. Please quote the above reference number for all queries relating to this study.

PLEASE NOTE: Research data should be securely stored in the school/department for a period of 5 years

[redacted]

.....
Dr Rosemary Sibanda (Chair)

/dd

Cc Supervisor: Professor Manoj Maharaj
cc Academic Leader Research: Professor Brian McArthur
cc School Administrator: Ms Angela Pearce

Humanities & Social Sciences Research Ethics Committee
Dr Rosemary Sibanda (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses: Edgewood Howard College Medical School Pietermaritzburg Westville