DEVELOPMENT OF AN INTEGRATED CYBERSECURITY FRAMEWORK FOR MITIGATING ONLINE IDENTITY THEFT AND PHISHING AMONG YOUTH IN WESTLANDS CONSTITUENCY, NAIROBI COUNTY.

ALICE KEMUNTO OGORO

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER INFORMATION SYSTEMS OF KENYA METHODIST UNIVERSITY.

OCTOBER, 2026

DECLARATION

I declare that this thesis is my original work and has not been presented in any other university.

Signature Date.03/10/2026

Alice Kemunto Ogoro

CIS-3-3466-3/2023

This thesis has been submitted for examination with our approval as university supervisors

Signature Date: 03/10/2026

Robert Murungi

Kenya Methodist University

Signature Date :03/10/2026

Jenu John

Kenya Methodist University

DEDICATION

I dedicate this thesis to my beloved family, whose unwavering support, encouragement, and sacrifices have been the foundation of my academic journey. To my parents, for their endless love and guidance; to my children, Ian, Jayden and Daisy, whose smiles inspire me to strive for excellence, and to my love, whose belief in me has been a constant source of motivation.

I also extend my dedication to my supervisors, mentors, lecturers, and colleagues, whose invaluable insights and encouragement have shaped my understanding and passion for knowledge.

ACKNOWLEDGEMENT

I am deeply grateful to God for the far He has brought me in my academic journey. His grace and guidance have been my source of strength and perseverance throughout this pursuit. I sincerely thank Kenya Methodist University for providing me with the opportunity to advance my studies and grow both academically and professionally. My heartfelt appreciation goes to my dedicated supervisors, Dr. Robert Murungi and Miss Jenu John, whose exceptional guidance, encouragement, and insightful feedback have been instrumental in shaping this research thesis. Their mentorship has greatly enriched my academic experience.

ABSTRACT

The rapid expansion of digital platforms in communication, finance, education, and public services has heightened exposure to cyber threats, with online identity theft and phishing emerging as major risks. Despite the existence of legal frameworks and cybersecurity awareness initiatives in Kenya, urban youth remain exposed to increasingly sophisticated cyber threats. This study examined the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County. Guided by Routine Activity Theory, the Health Belief Model, Protection Motivation Theory, and Institutional Theory, the study specifically examined the relationship between technology adoption and mitigation of identity theft and phishing; assessed the relationship between cybersecurity education and mitigation; examined the relationship between policy awareness and mitigation; determined the joint predictive contribution of the three factors; and developed a proposed empirically informed cybersecurity framework. The study adopted a descriptive correlational research design with qualitative supplementation and was predominantly quantitative. From a target population of 116,798 youth aged 18–35 years, a sample of 399 respondents was determined, of whom 338 participated in the study, representing a response rate of 84.7%. Data were collected using a structured questionnaire containing closed- and open-ended questions and supplemented by document review. Quantitative data were analysed using descriptive statistics, Pearson correlation analysis, and multiple regression analysis, while qualitative responses were analysed thematically. The findings showed positive and statistically significant relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing. Cybersecurity education had the strongest standardized predictive contribution, followed by technology adoption and policy awareness. Collectively, technology adoption, cybersecurity education, and policy awareness significantly predicted mitigation of identity theft and phishing, explaining 52.0% of the variation in mitigation outcomes ($R^2 = .520$, $F(3, 334) = 120.611$, $p < .001$). Based on these findings, the study developed a proposed empirically informed cybersecurity framework integrating technological safeguards, cybersecurity education, and policy awareness for mitigating online identity theft and phishing among youth in Westlands Constituency. The study concludes that the three dimensions provide complementary contributions to understanding mitigation and recommends strengthening practical cybersecurity education, promoting accessible and user-friendly security technologies, and enhancing awareness of cybercrime policies and reporting mechanisms. The study contributes to knowledge by integrating technological, educational, and policy dimensions within a context-specific framework for understanding the mitigation of online identity theft and phishing among urban youth.

TABLE OF CONTENTS

DECLARATION ..... **ii**
Kenya Methodist UniversityDEDICATION ..... **ii**
ACKNOWLEDGEMENT ..... **iv**
ABSTRACT ..... **v**
TABLE OF CONTENTS ..... **vi**
LIST OF TABLES ..... **ix**
LIST OF FIGURES ..... **x**
ABBREVIATIONS AND ACRONYMS ..... **xi**
CHAPTER ONE: INTRODUCTION **1**
1.1 Background of the Study 1
1.2 Statement of the Problem 6
1.3 Purpose of the Study 8
1.4 Objectives of the Study 8
1.5 Research Questions 9
1.6 Justification of the Study 10
1.7 Limitations of the study 11
1.8 Delimitation of the Study 12
1.9 Significance of the Study 14
1.10 Assumptions of the study 15
1.11 Operational Definition of Terms 16
CHAPTER TWO: LITERATURE REVIEW **19**
2.1 Introduction 19
2.2 Theoretical Review 19
2.3 Review of Empirical Literature 27
2.4 Knowledge Gaps 44
2.5 Summary of the Reviewed Literature 49
2.6 Conceptual Framework 53
CHAPTER THREE: RESEARCH METHODOLOGY **57**
3.1 Introduction 57

3.2 Research Design 58
3.3 Target Population 59
3.4 Sampling Technique and Sample Size 60
3.5 Data Collection Instruments 63
3.6 Data Collection Procedures 66
3.7 Pilot Study 68
3.8 Validity and Reliability of Research Instruments 69
3.9 Data Analysis Techniques and Presentation 70
3.10 Ethical Considerations 75
CHAPTER FOUR: RESULTS AND DISCUSSION 77
4.1 Introduction 77
4.2 Response Rate 77
4.3 Pilot Test Results 78
4.4 Demographic Characteristics of Respondents 81
4.5 Technology Adoption and Mitigation of Online Identity Theft and Phishing 84
4.6 Cybersecurity Education and Mitigation of Online Identity Theft and Phishing 91
4.7 Policy Awareness and Mitigation of Online Identity Theft and Phishing 97
4.8 Joint Predictive Contribution of Technology Adoption, Cybersecurity Education, and Policy Awareness to Mitigation 105
4.9 Development of a Cybersecurity Framework for Mitigating Identity Theft and Phishing 107
4.10 Discussion of Findings 112
4.11 Summary of the Chapter 121
CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 123
5.1 Introduction 123
5.2 Summary of the Study 123
5.3 Conclusions 125
5.4 Recommendations 127
5.5 Limitations of the Study 129

5.6 Contribution to Knowledge 130
REFERENCES..... 131
APPENDICES..... 140
Appendix I: Consent Form 140
Appendix II: Questionnaire 143
Appendix III: Document Review Guide for Secondary Data Collection 147
Appendix IV: Research Permit 148

LIST OF TABLES

Table 4. 1: Response Rate 78
Table 4. 2: Content Validity Results 79
Table 4. 3: Reliability Test Results 80
Table 4. 4: Demographic Characteristics of Respondents 81
Table 4. 5: Perceived Effectiveness of Mitigation Strategies (n = 338) 83
Table 4. 6: Descriptive Statistics for Technology Adoption 86
Table 4. 7: Correlation between Technology Adoption and Mitigation 87
Table 4. 8: Regression Results on Technology Adoption and Mitigation of Identity Theft & Phishing 88
Table 4. 9: Descriptive Statistics for Cybersecurity Education (n = 338) 92
Table 4. 10: Correlation between Cybersecurity Education and Mitigation 94
Table 4. 11: Regression Results on Cybersecurity Education on Mitigation 95
Table 4. 12: Descriptive Statistics for Policy Awareness 99
Table 4. 13: Correlation between Policy Awareness and Mitigation 101
Table 4. 14: Regression Results on the Predictive Relationship between Policy Awareness and Mitigation 102
Table 4. 15: Regression Results on the Integrated Predictive Contribution of Technology Adoption, Cybersecurity Education, and Policy Awareness to Mitigation 105

LIST OF FIGURES

Figure 2. 1: Conceptual Framework 56

Figure 4. 1: Cybersecurity Framework for Mitigating Identity Theft and Phishing.... 111

ABBREVIATIONS AND ACRONYMS

2FA	Two-Factor Authentication
CAK	Communications Authority of Kenya
CMCA	Computer Misuse and Cybercrimes Act
DPA	Data Protection Act
HBM	Health Belief Model (Rosenstock, 1974)
ICT	Information and Communication Technology
KEMU	Kenya Methodist University
KNBS	Kenya National Bureau of Statistics
NCRC	National Crime Research Centre
RAT	Routine Activity Theory (Cohen & Felson, 1979)
SPSS	Statistical Package for the Social Sciences
PMT	Protection Motivation Theory (Rogers, 1975)

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Cybersecurity refers to the practices, technologies, behaviors, and institutional safeguards that protect users and digital systems from unauthorized access, attacks, or exploitation (European Union Agency for Cybersecurity [ENISA], 2023). In this study, cybersecurity specifically concerns the capacity of youth to protect their personal data and digital identities from online threats particularly phishing and identity theft. It encompasses not only technical tools such as firewalls, secure browsing, and multi-factor authentication but also individual awareness, digital habits, and the effectiveness of legal and policy frameworks intended to prevent, detect, and respond to such crimes (International Telecommunication Union [ITU], 2024; Mbaya & Muriuki, 2023).

Among the most pervasive threats within this domain are phishing and online identity theft. Phishing refers to a manipulative cyber tactic that deceives users into revealing confidential details like login credentials or banking information by masquerading as legitimate sources through emails, fake websites, or text messages (Putra et al., 2024). Digital identity theft entails illegally obtaining and misusing an individual's personal or financial information to assume their identity, commit fraud, or exploit them in other ways. These threats exploit both technological weaknesses and human behavior, making them difficult to control through technology alone.

The global surge in digitization has transformed nearly every aspect of modern life, from how individuals communicate to how institutions manage critical operations (Desetty et

al. 2020). Digital platforms are now deeply embedded in everyday processes such as online banking, e-commerce, remote education, telehealth, and governance. This digital shift has generated immense benefits greater accessibility, speed, and efficiency but has also introduced new, complex vulnerabilities that cybercriminals have been quick to exploit. With the growing dependence on digital platforms for storing and sharing personal information, cyber threats like phishing and identity theft have surged in frequency, complexity, and severity. As reported by Cybersecurity Ventures (2023), global cybercrime is expected to inflict financial damages reaching USD 10.5 trillion each year by 2025 an alarming rise from USD 3 trillion in 2015 with crimes tied to identity being among the most rapidly expanding types.

In the African context, the situation is particularly concerning. While the region has made significant strides in digital adoption especially in mobile internet usage and fintech innovation its cybersecurity capacity remains underdeveloped. The International Telecommunication Union (ITU, 2024) highlights that Africa ranks the lowest on the Global Cybersecurity Index, citing major gaps in legal frameworks, institutional coordination, and public awareness. A report by the African Union Commission (2024) confirms that phishing is the most commonly reported cybercrime on the continent, disproportionately targeting youth populations who are highly active online but often lack the technical literacy or tools to protect themselves. Urban youth are especially vulnerable due to their heavy reliance on social media, mobile applications, and digital job markets all of which are common entry points for cybercriminals.

A growing body of local evidence highlights the severity of cybersecurity risks facing Kenyan digital users, including youth. Kenya continues to experience substantial growth in detected cyber threats as the use of digital platforms expands. According to the Communications Authority of Kenya (CA, 2024), detected cyber threats increased from 855,554,988 in the 2022/2023 financial year to 3,449,333,823 in 2023/2024. These trends demonstrate the scale of cybersecurity threats within Kenya's expanding digital environment and reinforce the need for effective technological, educational, and institutional measures for protecting users against threats such as phishing and online identity theft.

Kenya stands at the heart of Africa's digital transformation, with widespread use of mobile financial services, digital government platforms, e-commerce, social networking, and other internet-based services. However, increased digital participation has also expanded users' exposure to cybersecurity threats. Young people are particularly relevant in this environment because of their extensive engagement with mobile applications, social media, online learning, digital financial services, and other internet-based platforms. Their level of protection therefore depends not only on access to technology but also on their adoption of appropriate cybersecurity practices, cybersecurity education, and awareness of available legal and policy protections.

The youth demographic represents the most digitally engaged age cohort in Kenya. According to the African Union and the Kenyan National Youth Policy, youth are individuals aged 18 to 35, a period characterized by increased autonomy, technological adoption, and economic participation. This group forms a significant portion of mobile

internet subscribers, digital content creators, and freelance workers (CAK, 2023; Kenya National Bureau of Statistics [KNBS], 2024). However, their frequent and intensive use of digital platforms is not matched by equivalent cybersecurity awareness or access to protective tools (Sitienei, 2025). As a result, their high exposure levels, coupled with limited defensive capacity, place them at the forefront of identity-related cyber threats (Mbaya & Muriuki, 2023). This age group is therefore not only highly vulnerable but also central to the development of effective, youth-centered cybersecurity strategies (Deutsche Gesellschaft für Internationale Zusammenarbeit [GIZ], 2021; ITU, 2024).

Although Kenya has instituted progressive laws such as the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019), these legal instruments have not fully translated into effective protection on the ground. Studies by Mbaya and Muriuki (2023) and Sitienei (2025) point to significant challenges in implementation, ranging from limited public awareness campaigns to weak institutional enforcement and inadequate coordination among cybersecurity stakeholders. Additionally, many victims of cybercrime particularly youth do not report these incidents due to fear of blame, perceived ineffectiveness of legal processes, or lack of knowledge about how to seek redress.

Within this national picture, Westlands Constituency in Nairobi emerges as a critical focus area. A vibrant, cosmopolitan urban hub, Westlands is home to a diverse population with high levels of internet penetration, smartphone ownership, and digital engagement. Within this national picture, Westlands Constituency in Nairobi emerges as a critical focus area. A vibrant, cosmopolitan urban hub, Westlands is characterized by substantial engagement with internet-enabled services and digital platforms. However, this digital engagement

also exposes users to cybersecurity risks. Complementing these findings, evidence from studies on cybercrime in Kenya indicates that digitally active users remain exposed to cyber threats, particularly where cybersecurity awareness and access to protective technologies are limited (Mbaya & Muriuki, 2023).

This study was anchored in four complementary theoretical perspectives, with Routine Activity Theory (Rat et al., 1979) providing the overarching theoretical perspective. RAT proposes that criminal activity becomes more likely when a motivated offender encounters a suitable target in the absence of capable guardianship. Applied to the digital context, the theory helps explain the vulnerability of youth who are highly active online but may lack adequate technological safeguards, cybersecurity knowledge, or other forms of digital guardianship.

Protection Motivation Theory (PMT) Rogers, (1975) and the Health Belief Model (HBM) Rosenstock, (1974) provided complementary behavioural perspectives for understanding protective responses to cybersecurity threats. PMT explains protective behaviour through threat appraisal and coping appraisal, while HBM emphasizes perceived susceptibility, perceived severity, and individuals' willingness to undertake preventive actions. These perspectives were relevant to understanding cybersecurity education and protective responses among youth but were not treated as separate variables or mediators in the empirical model.

Institutional Theory DiMaggio and Powell (1983) provided the institutional perspective relevant to policy awareness. The theory was useful in understanding the role of formal

laws, regulatory mechanisms, institutional enforcement, and public awareness in shaping the environment within which individuals respond to cybersecurity threats. In this study, this perspective was particularly relevant to awareness of cybercrime and data-protection laws, perceptions of policy enforcement, and trust in institutional responses.

Together, the theories provided a multidimensional basis for examining the relationships between technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing among youth in Westlands Constituency. The theoretical perspectives also provided a basis for interpreting the empirical findings that informed the development of the proposed integrated cybersecurity framework.

1.2 Statement of the Problem

Despite Kenya's legal and policy mechanisms for addressing cybercrime, online identity theft and phishing remain significant cybersecurity concerns. Kenya has established the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and the National Cybersecurity Strategy 2022–2027 to strengthen cybersecurity governance, regulation, capacity development, and cyber-risk reduction (National Computer and Cybercrimes Coordination Committee [NC4], 2022). Nevertheless, detected cyber threats increased from 855,554,988 in 2022/2023 to 3,449,333,823 in 2023/2024 (Communications Authority of Kenya [CA], 2024). This persistence of cyber threats demonstrates the continuing need to strengthen protection at both institutional and individual-user levels.

Existing cybersecurity responses include technological safeguards, cybersecurity education, and legal and policy mechanisms. However, these approaches are often addressed separately, yet cybersecurity awareness does not necessarily translate into appropriate protective behaviour (Bognár & Bottyán, 2024), while phishing continues to exploit human and behavioural vulnerabilities (Morrow, 2024). Moreover, the National Cybersecurity Strategy 2022–2027 provides a broad national framework rather than a context-specific framework addressing how youth adopt protective technologies, acquire cybersecurity education, and understand relevant cybersecurity policies (NC4, 2022). Consequently, the national framework does not specifically explain how these dimensions relate to mitigation practices against online identity theft and phishing among youth in Westlands Constituency.

The specific empirical problem is the limited localized evidence on the individual and joint relationships between technology adoption, cybersecurity education, policy awareness, and Mitigation of Identity Theft & Phishing among youth in Westlands Constituency. Existing research and frameworks have largely addressed technological, educational, behavioural, or institutional dimensions separately, leaving limited understanding of how these dimensions operate together within this specific urban context (Bognár & Bottyán, 2024; Morrow, 2024). This study therefore examined these relationships and integrated the empirical findings to inform the development of an empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

1.3 Purpose of the Study

The purpose of this study was to develop a proposed empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency, Nairobi County. Specifically, the study examined the relationships between technology adoption, cybersecurity education, policy awareness, and perceived effectiveness of mitigation strategies against online identity theft and phishing. Technology adoption encompassed protective practices such as multi-factor authentication, strong password management, secure browsing, and phishing-detection measures, while cybersecurity education focused on knowledge and skills for recognizing and responding to online threats. Policy awareness addressed youths' knowledge and understanding of relevant cybersecurity and data protection provisions. The study further examined the joint predictive contribution of technology adoption, cybersecurity education, and policy awareness to mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies). The findings from these dimensions were subsequently integrated to inform the development of the proposed cybersecurity framework.

1.4 Objectives of the Study

1.4.1 Main Objective

To develop a proposed empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

1.4.2 Specific Objectives

i. To determine the relationship between technology adoption and mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

ii. To determine the relationship between cybersecurity education and mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

iii. To determine the relationship between policy awareness and mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

iv. To determine the extent to which technology adoption, cybersecurity education, and policy awareness jointly predict mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

v. To develop a proposed empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency, Nairobi County based on the empirical findings of the study.

1.5 Research Questions

i. What relationship exists between technology adoption and Mitigation of Identity Theft & Phishing among youth in Westlands Constituency, Nairobi County?

ii. What relationship exists between cybersecurity education and Mitigation of Identity Theft & Phishing among youth in Westlands Constituency, Nairobi County?

iii. What relationship exists between policy awareness and Mitigation of Identity Theft & Phishing among youth in Westlands Constituency, Nairobi County?

iv. To what extent do technology adoption, cybersecurity education, and policy awareness jointly predict Mitigation of Identity Theft & Phishing among youth in Westlands Constituency, Nairobi County?

v. What components and relationships should constitute a proposed empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency, Nairobi County?

1.6 Justification of the Study

Online identity theft and phishing continue to undermine Kenya's digital progress, with youth in urban areas like Westlands particularly vulnerable due to their high reliance on mobile money, gig platforms, and social media (KNBS, 2024). Despite legislative efforts such as the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019), cyber incidents targeting youth remain high, exposing enforcement gaps, low awareness, and fragmented intervention strategies (CAK, 2023; Sitienei, 2025).

This study was necessary to address critical gaps in current research and practice. Empirical data on how urban youth perceive and respond to cyber risks in Kenya was limited. Most existing literature emphasizes technical or legal dimensions, overlooking

behavioral factors and lived user experiences (Baharuddin et al., 2025; Mbaya & Muriuki, 2023). Furthermore, few studies adopted an integrated framework that connects user behavior, education, and institutional structures.

By focusing on youth, Kenya's most digitally active but under protected demographic (GIZ, 2021; ITU, 2024) this study offered a multidimensional model to inform more inclusive cybersecurity strategies. Its findings supported youth-targeted education, improve institutional responsiveness, and contribute to policy reforms grounded in context-specific realities.

1.7 Limitations of the study

There was a scarcity of integrated academic research that simultaneously examined technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among urban youth in contexts such as Westlands Constituency, which may constrain comparative analysis during the literature review. To mitigate this, the study prioritized primary data collection from the target population and complement it with regional and global empirical analogs to enrich contextual relevance. Second, access to sensitive cybersecurity data such as anonymized breach reports, institutional threat logs, or internal response metrics may be restricted due to privacy regulations or organizational reluctance. To overcome this, the researcher obtained all necessary ethical approvals from relevant review boards and requested formal institutional permissions. Where direct access was denied, the study relied on public domain reports, official statistics, and participant self-reporting.

Third, due to time constraints linked to academic calendar timelines, the duration of fieldwork may limit the frequency or geographic spread of in-person data collection. This limitation was addressed through purposive sampling and the use of digitally administered surveys, allowing for greater reach and efficiency without compromising data quality. Fourth, the sensitive nature of cybercrime-related experiences may result in non-responsiveness or partial disclosure by participants. To build trust and improve participation, the researcher implemented strict anonymity and confidentiality protocols, including coded identifiers, password-protected storage, and transparent consent procedures. Emphasis was placed on participants' voluntary engagement, and the data collection instruments were designed to minimize psychological discomfort.

Finally, the study was limited in its ability to empirically test advanced cybersecurity technologies (e.g., phishing simulators or intrusion detection systems) due to the lack of technical infrastructure and software licensing. To address this, the study focused on perception-based and behavioral data, and used secondary literature to support the evaluation of technological responses.

1.8 Delimitation of the Study

This study was geographically delimited to Westlands Constituency in Nairobi County, Kenya, an urban area characterized by high levels of digital access and youth engagement with online services. The target population was youth (i.e., aged 18 to 35 years), who are active internet users. This demographic was selected due to its disproportionate exposure

to digital threats like phishing and identity theft and its strategic significance in shaping Kenya's digital resilience.

Thematically, the study focused solely on online identity theft and phishing, two of the most prevalent and impactful forms of cybercrime affecting individuals in Kenya's digital ecosystem. Other forms of cybercrime such as ransomware, cyberbullying, and financial fraud were excluded to maintain conceptual clarity and focus. The chosen scope reflected the urgent need to explore these two threats, which are especially common among urban youth, yet under-researched at the behavioral and policy interaction level.

Methodologically, the study adopted a descriptive correlational research design to explore relationships among technology adoption, cybersecurity education, policy awareness, and Mitigation of Identity Theft & Phishing. A semi-structured questionnaire was used to collect both quantitative and qualitative data from a purposively selected sample of youth in Westlands. The questionnaire was designed to capture not only behavioral trends and awareness levels but also individual perceptions and experiences with cyber threats. In addition, the study incorporated a document review of relevant national cybersecurity policies, strategic frameworks, and public reports to contextualize the findings and assess alignment between policy intentions and user-level realities.

The study did not include technical testing or forensic analysis of digital systems, nor did it evaluate corporate or institutional cybersecurity infrastructures beyond their influence on individuals. By clearly delimiting its geographical focus, target population, thematic boundaries, and data sources, the study aimed to generate evidence-based insights tailored

to Kenya's urban youth and usable by policymakers, educators, and community organizations.

1.9 Significance of the Study

This study holds significant relevance for advancing digital safety and resilience among urban youth in Kenya. By examining the relationships between technology adoption, cybersecurity education, policy awareness, and Mitigation of Identity Theft & Phishing, the study provides empirical evidence on factors associated with safer online practices among youth.

For policymakers and regulatory authorities, the study provides empirical evidence on the relationship between cybersecurity legislation and youth awareness, behaviour, and protective practices. The statistical findings, particularly the correlation and regression results, identify the factors associated with and predictive of mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies). These findings may inform interventions such as targeted youth awareness campaigns, improved policy implementation, and more accessible communication of digital rights and responsibilities under Kenya's cybercrime and data protection laws.

For educators, training institutions, and digital literacy programmes, the findings provide evidence on the relationship between cybersecurity education and mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies). The findings may inform the development of curriculum content, community-based initiatives, and training programmes that address identified cybersecurity knowledge and skills gaps among youth.

For technology developers and cybersecurity practitioners, the study provides evidence on youth adoption of protective practices such as multi-factor authentication, secure browsing, password management, and phishing-detection measures. Understanding these practices and the challenges associated with their adoption may inform the development of more accessible and user-centred cybersecurity tools for young users.

The study further contributes to youth digital safety by providing evidence on cybersecurity awareness, protective practices, incident reporting, and relevant legal protections. The proposed empirically informed cybersecurity framework integrates the technological, educational, and policy dimensions examined in the study and identifies their relationships with mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies).

Beyond its application to Westlands Constituency, the proposed empirically informed cybersecurity framework may provide a basis for further research and adaptation in other urban settings. Since the framework was developed from the empirical findings of this study and was not independently validated, its application to other populations and contexts would require further assessment.

1.10 Assumptions of the study

First, it was assumed that respondents provided honest, complete, and thoughtful responses to both quantitative and qualitative questions during data collection. This assumption was grounded in the expectation that the research setting characterized by strict confidentiality protocols, anonymity assurances, and informed consent encouraged

openness and reduce social desirability bias. Second, it was assumed that the purposively selected participants possessed the characteristics required for inclusion in the study and provided information relevant to the study objectives.

Third, it was assumed that participants understood the questions as intended, particularly those related to technology adoption, cybersecurity education, policy awareness, and Mitigation of Identity Theft & Phishing. To reduce the risk of misunderstanding, the questionnaire underwent a preliminary trial with a limited group, allowing for revisions based on participant feedback before administration in the main study. Fourth, the study assumed that the descriptive correlational research design with qualitative supplementation was suitable for examining the relationships among the study variables.

Finally, it was assumed that all ethical guidelines governing research involving human participants were upheld throughout the study. These included securing informed consent, protecting participant privacy, and ensuring voluntary participation. By embedding ethical rigor and transparent procedures at every stage, the study aimed to reduce bias, build trust, and enhance data integrity.

1.11 Operational Definition of Terms

Cybersecurity Education: A structured process designed to enhance individuals' knowledge, attitudes, and practical skills in identifying, preventing, and responding to cyber threats, including phishing and online fraud. It includes formal training, awareness campaigns, and informal learning activities targeted at promoting digital safety (Ismaeel, 2025).

Cybersecurity Tools are software applications and digital technologies developed to identify, counteract, or manage cyber risks. These include protective systems such as antivirus software, firewalls, encryption technologies, and intrusion detection tools, all aimed at securing sensitive data and facilitating safe online activities (Girma et al., 2024).

Digital Literacy involves the competence to navigate, assess, and utilize digital platforms and resources in a secure and efficient manner. In the context of this study, it includes awareness of cyber risks, safe online practices, and knowledge of digital rights (UNESCO, 2023).

Identity Theft: The unauthorized acquisition and use of someone's personal or financial data such as identification numbers, login credentials, or banking details typically for fraudulent gain or criminal impersonation. It often occurs through methods like phishing and data breaches (Obiokafor, 2024).

Mitigation: In this study, mitigation refers to the reduction in frequency, severity, and consequences of phishing and identity theft through targeted interventions. These include the adoption of cybersecurity tools, behavior change through education, and enhanced institutional support in urban settings like Westlands (Ogunola et al., 2024).

Phishing is a fraudulent online strategy that deceives people into disclosing private information like login credentials or credit card numbers by pretending to be legitimate entities through counterfeit emails, messages, or websites. It is a frequent method used to launch identity-related attacks (Putra et al., 2024).

Policy Awareness: In this study, policy awareness refers to youths' awareness and understanding of relevant cybersecurity and data-protection laws and institutional mechanisms (Waliullah et al., 2025). It encompasses awareness of cybercrime and data-protection legislation, perceptions of policy enforcement, and trust in institutional responses to cybercrime.

Social Engineering refers to the use of psychological tactics by cybercriminals to manipulate individuals into giving away sensitive data or engaging in risky digital behavior. Techniques such as phishing, baiting, and pretexting fall under this umbrella, relying on deception rather than technical intrusion (Parsons et al., 2022).

Technology Adoption involves individuals incorporating cybersecurity solutions, like antivirus tools, password management systems, secure browsing platforms, and multi-factor authentication, into their digital routines to defend against threats such as phishing and identity fraud (Girma et al., 2024).

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

In this chapter, literature on mitigating online identity theft and phishing among urban youth in Westlands Constituency is reviewed. Youth are especially vulnerable due to high digital engagement and low cybersecurity preparedness (Putra et al., 2024). The review goes beyond summarizing existing work by analyzing the applicability and limitations of key theories and empirical studies in the Kenyan context. Section 2.2 discusses Routine Activity Theory (Cohen & Felson, 1979) (RAT), the Health Belief Model (Rosenstock, 1974) (HBM), and Institutional Theory DiMaggio and Powell, (1983), examining how each explains youth vulnerability. Section 2.3 evaluates empirical evidence on technology use, cybersecurity education, and policy awareness, identifying inconsistencies and gaps in current approaches. Section 2.4 outlines specific knowledge and methodological gaps, while Section 2.5 summarizes key insights. Section 2.6 presents the conceptual framework, which integrates theoretical and empirical findings to support a locally relevant, youth-focused mitigation model.

2.2 Theoretical Review

This study was grounded in multiple theories aligned with the variables under investigation, with Routine Activity Theory (RAT) providing the overarching explanatory perspective. Protection Motivation Theory (PMT) and the Health Belief Model (HBM) provided complementary behavioural perspectives relevant to cybersecurity education and protective behaviour, while Institutional Theory provided the institutional perspective

relevant to policy awareness. Together, the theories provided a multidimensional basis for examining the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency.

2.2.1 Routine Activity Theory

Routine Activity Theory (RAT), introduced by Cohen and Felson (1979), provides a situational perspective for analyzing criminal behavior by emphasizing the role of environmental and social conditions rather than the offender's intent. The theory posits that a crime is most likely to take place when three factors align at the same time and location: a motivated offender, a suitable target, and the absence of capable guardianship. Originally developed during a period of escalating urban crime in the United States, RAT has since been extended to cybercrime, where it provides insight into the situational and behavioral dynamics associated with online offenses such as phishing, identity fraud, cyberstalking, and digital scams.

In digital spaces, the components of RAT are reconceptualized. The motivated offender is a cybercriminal seeking to exploit vulnerabilities, while the suitable target includes internet users whose online activities expose them to potential cyber threats. Capable guardianship extends beyond physical protection to encompass digital safeguards such as antivirus software, firewalls, secure platforms, institutional policies, and informed user behavior. In this study, RAT was applied to understand how the online activities of youth

in Westlands Constituency and the presence or absence of technological and behavioural safeguards relate to their exposure and responses to online identity theft and phishing.

Empirical studies have demonstrated the applicability of RAT to cybercrime. Goncalves (2024) found that during the COVID-19 lockdowns, increased periods of online activity created greater opportunities for cyber fraud, illustrating how changes in routine behavior may heighten exposure to digital offenders. Similarly, Al-Badayneh et al. (2024) demonstrated the relevance of awareness of digital security policies in understanding cybercrime victimization. These findings reinforce the importance of exposure and capable guardianship in understanding online cybersecurity risks.

Despite its strengths, RAT has limitations when applied to complex cybersecurity behaviour. The theory primarily explains the situational conditions under which opportunities for victimization arise but provides limited explanation of why individuals exposed to similar threats may differ in their risk perceptions, knowledge, self-efficacy, and protective responses. Holt and Bossler (2016) further observe that routine activity explanations of cybercrime may not fully capture broader economic, infrastructural, and educational factors that shape digital guardianship. These limitations are particularly relevant where individuals differ in access to technologies, cybersecurity knowledge, and institutional support.

To address these limitations, the study complemented RAT with the Health Belief Model (Rosenstock, 1974), Protection Motivation Theory (Rogers, 1975), and Institutional Theory (DiMaggio & Powell, 1983). While RAT accounts primarily for environmental

opportunity and guardianship, HBM and PMT provide behavioural and cognitive explanations of risk perception and protective responses, while Institutional Theory addresses the broader legal and institutional environment.

RAT therefore provided the overarching theoretical perspective for the study. Technology adoption can be understood as one form of digital guardianship, while cybersecurity education may strengthen individuals' capacity to recognize and respond to potential threats. Policy and institutional mechanisms provide a broader form of formal guardianship. RAT consequently provided the overarching foundation within which the technological, educational, and policy dimensions of the study were integrated.

2.2.2 Protection Motivation Theory

Protection Motivation Theory (PMT), originally proposed by Rogers (1975) and later expanded in 1983, is a psychological framework for explaining why individuals adopt self-protective behaviors when confronted with threats. The theory focuses on two core cognitive processes: threat appraisal and coping appraisal. Threat appraisal concerns the perceived severity of a threat and an individual's perceived vulnerability to it, while coping appraisal involves the effectiveness of the proposed protective response, self-efficacy, and the costs associated with undertaking that response (Rogers, 1983).

In cybersecurity research, PMT has been applied to understand decisions concerning protective practices such as multi-factor authentication, cautious browsing, and avoidance of suspicious links. Zainal (2022), for example, found that perceived seriousness of cyber threats and self-efficacy were important in explaining self-protective digital behaviour

among university students. Similarly, Chan-Tin et al. (2022) reported that individuals with stronger perceptions of cybercrime threats and greater belief in the effectiveness of mitigation strategies were more likely to adopt secure digital practices.

PMT is particularly relevant because cybersecurity behaviour involves more than the availability of technological safeguards. Individuals must recognize a threat and believe that they possess the knowledge and ability to undertake an appropriate protective response. Previous research has also demonstrated that factors such as fear of potential loss and other consequences can shape responses to phishing and identity-related threats (Desolda et al., 2021). Educational exposure may further strengthen knowledge and confidence in undertaking protective action.

In this study, PMT provided a behavioural explanation for the relationship between cybersecurity education and mitigation of online identity theft and phishing. The theory was relevant to questionnaire measures concerning cybersecurity training, identification of phishing messages, knowledge of reporting channels, and confidence in avoiding online identity theft. Rather than treating PMT constructs as separate variables in the statistical model, the theory provided a behavioural basis for understanding why differences in cybersecurity knowledge and preparedness may be associated with differences in mitigation.

A limitation of PMT is its emphasis on individual cognitive appraisal, which does not fully account for the situational and institutional environments within which cybersecurity behaviour occurs. RAT complemented PMT by addressing exposure and guardianship,

while Institutional Theory accounted for formal legal and institutional mechanisms. PMT was therefore applied as a complementary behavioural perspective within the study's broader theoretical framework.

2.2.3 Health Belief Model

The Health Belief Model (HBM), associated with Rosenstock (1974), was initially developed to understand and predict preventive health behavior based on individuals' perceptions and attitudes. The model proposes that individuals are more likely to undertake preventive action when they perceive themselves as susceptible to a threat, regard its consequences as serious, recognize the benefits of protective action, perceive manageable barriers to acting, and possess sufficient self-efficacy. Protective behavior may also be stimulated by cues to action (Glanz et al., 2008). Although initially developed within health contexts, HBM has subsequently been extended to cybersecurity and other forms of preventive digital behavior (Baral, 2021; Du et al., 2024).

Recent research demonstrates the model's relevance to cybersecurity behaviour. Du et al. (2024) found that perceived susceptibility to phishing and perceived severity of identity theft were associated with the adoption of preventive behaviours such as multi-factor authentication and secure password management. Such findings demonstrate the relevance of individual risk perceptions when seeking to understand why awareness of cybersecurity threats may or may not translate into protective action.

HBM is particularly useful in explaining the cognitive dimensions associated with cybersecurity education. Individuals may possess information about phishing and identity

theft but differ in their perceptions of vulnerability, confidence in responding, and perceived barriers to taking protective action. The model therefore complements PMT by emphasizing perceived susceptibility, severity, barriers, and cues to action in understanding preventive behaviour.

In this study, HBM provided a complementary lens for understanding the behavioural and cognitive dimensions associated with cybersecurity education and mitigation. It was particularly relevant to understanding awareness of cyber risks, confidence in avoiding identity theft, and concern about personal data being stolen online. However, HBM constructs were not treated as separate independent or mediating variables in the statistical model. Instead, the model provided theoretical support for interpreting the behavioural and cognitive dimensions captured by the questionnaire.

Despite its strengths, HBM has limitations. Critics argue that its emphasis on individual perceptions and rational decision-making may overlook emotional, social, and environmental factors influencing behavior (Esteves, 2023). It may also provide limited explanation of habitual online behavior and rapidly changing digital threats that do not always involve deliberate risk appraisal. In this study, these limitations were addressed by RAT, which provided the situational perspective, and Institutional Theory, which incorporated the broader policy and institutional environment.

2.2.4 Institutional Theory

Institutional Theory, initially advanced by Meyer and Rowan (1977) and further developed by DiMaggio and Powell (1983), argues that individual and organizational

actions are influenced by established regulations, societal norms, and institutional pressures. Rather than behavior being determined exclusively by individual efficiency considerations, actors operate within institutional environments characterized by formal rules, normative expectations, and expectations of legitimacy (DiMaggio & Powell, 1983; Scott, 2014).

In cybersecurity, Institutional Theory provides a useful perspective for understanding how regulatory frameworks, institutional expectations, enforcement mechanisms, and institutional legitimacy shape cybersecurity compliance and behavior. Delso-Vicente et al. (2025), for example, established that institutional culture and leadership commitment were important to cybersecurity compliance in Spanish universities. These findings demonstrate that cybersecurity practices are shaped not only by individual knowledge and technological capability but also by the institutional environment.

Within Kenya, cybersecurity behaviour occurs within a formal institutional environment that includes the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and associated cybersecurity governance and reporting mechanisms. Institutional Theory therefore provides a basis for understanding how awareness of legal frameworks, perceptions of enforcement, and confidence in relevant institutions may relate to how youth understand and respond to cybersecurity threats.

Institutional Theory, however, is not without limitations. Its emphasis on institutional pressures can understate individual agency, resistance, and localized interpretation of institutional expectations (Greenwood et al., 2017). It may also inadequately account for

differences in access to digital infrastructure and informal influences that shape how formal policies are understood and acted upon. These limitations make it necessary to complement the institutional perspective with theories addressing individual behaviour and situational exposure.

In this study, Institutional Theory informed the independent variable policy awareness. Specifically, it provided a theoretical basis for examining awareness of cybercrime and data-protection laws, perceptions of policy enforcement, and trust in institutional responses to reported cybercrime. Institutional Theory therefore complemented RAT, PMT, and HBM by incorporating the formal institutional dimension into the integrated theoretical explanation of the mitigation of online identity theft and phishing among youth in Westlands Constituency.

2.3 Review of Empirical Literature

Empirical studies directly relate to the study variables: technology adoption, cybersecurity education, policy awareness, and online identity theft and phishing are reviewed in sub-sections below. The focus is on identifying existing knowledge, highlighting key findings, and identifying gaps to be addressed. Particular attention was paid to studies conducted in the African context and among youth populations, as they are highly exposed to digital risks due to high engagement with technology and variations in cybersecurity knowledge and protective practices.

2.3.1 Technology Adoption

Technology adoption refers to the process through which individuals or institutions embrace, integrate, and consistently use digital innovations to enhance efficiency, productivity, and safety (Davis, 1989). In the realm of cybersecurity, adoption encompasses the use of tools such as antivirus software, firewalls, multi-factor authentication (MFA), virtual private networks (VPNs), spam filters, and password managers to detect, prevent, or respond to cyber threats like phishing, spoofing, and online identity theft (Afzal et al., 2024; Kabaya & Kageni, 2024). Crucially, adoption is not determined solely by access to technology but is shaped by a constellation of factors including perceived usefulness, usability, technical literacy, institutional support, trust, and behavioral intentions (Venkatesh et al., 2012; Zainal, 2022).

Routine Activity Theory (RAT), which provides the overarching theoretical perspective for this study, offers a useful basis for understanding technology adoption as a form of capable digital guardianship (Cohen & Felson, 1979). In the cybersecurity context, protective technologies such as antivirus software, firewalls, multi-factor authentication, secure browsing tools, and password-management practices can strengthen guardianship by reducing opportunities for successful phishing and identity theft. The relevance of such safeguards is particularly important among youth whose frequent engagement with digital platforms may increase exposure to motivated offenders where adequate protective measures are absent. Although technology-adoption models such as the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) emphasize factors such as perceived usefulness and ease of use (Venkatesh & Davis, 2000), the present study did not examine these constructs as a separate theoretical

model. Instead, technology adoption was examined primarily through the actual use of cybersecurity tools and protective practices, consistent with RAT's emphasis on capable guardianship. Nevertheless, usability and accessibility remain relevant practical considerations because security technologies that are difficult to use may be less consistently adopted, particularly among youth (Obiokafor, 2024).

Global empirical evidence underscores the behavioral nature of cybersecurity adoption. In the United Arab Emirates, Zainal (2022) employed a hybrid SEM-ANN approach using responses from over 300 mobile payment users. The study found that cybersecurity awareness and perceived behavioral control rather than perceived threat were the most influential factors in determining whether users adopted protective tools. This suggests that simply informing users of risks is insufficient; users must also feel empowered and capable of acting upon that information. In India, Afzal et al. (2024) applied PLS-SEM to a sample of 421 e-banking users and found low adoption of cybersecurity features such as secure login and OTP verification, despite high awareness. The primary barriers were poor user interface design, lack of confidence, and a dependence on institutional actors, such as banks, to manage security. Although the studies were conducted in different settings and employed different analytical approaches, both point to a gap between awareness of cybersecurity risk and actual adoption of protective technologies. Zainal (2022) places greater emphasis on behavioral control, whereas Afzal et al. (2024) highlights usability and dependence on institutional security. This suggests that technology adoption is shaped by both individual capability and the characteristics of the security tools themselves.

Across sub-Saharan Africa, regional studies reveal even more pronounced barriers. In Ghana, Jibril et al. (2020) applied the Technology Threat Avoidance Theory (TTAT) to assess security tool usage among 300 e-banking users. The study found that younger users were the least likely to adopt MFA or encryption, citing convenience, high perceived effort, and the cost of implementation. The researchers concluded that behavioral interventions, institutional endorsement, and publicly funded training programs were essential to stimulate adoption. In Tanzania, Mwamba and Mjema (2024) surveyed mobile users in Dar es Salaam and found that although 67% had encountered phishing attempts, only 12% used cybersecurity applications. Factors included language barriers, app complexity, and limited digital literacy, particularly among youth who accessed the internet through low-cost smartphones. The Ghanaian and Tanzanian findings are broadly consistent in showing low use of protective technologies, but they identify somewhat different constraints. Jibril et al. (2020) emphasize effort, convenience, and cost, while Mwamba and Mjema (2024) highlight language, device limitations, and digital literacy. These differences demonstrate why findings from one African context cannot automatically be generalized to digitally active youth in Westlands Constituency.

In Kenya, the pattern is similarly concerning. The National Crime Research Centre (Mbaya & Muriuki, 2023) reported that phishing, impersonation, and online scams were among the most reported cybercrimes, particularly in urban counties. Yet, the use of available protective tools remained low. The study noted that most urban youth were unaware of built-in security settings on their smartphones, had not enabled MFA, and often reused passwords across platforms. These findings were echoed by Sitienei (2025), who

found that MFA adoption on the eCitizen platform was predominantly reactive, triggered only after a data breach or identity theft had occurred. This behavior suggests that adoption of available safeguards may not occur consistently even among frequent users of digital platforms.

Additional insights from Kabaya and Kageni (2024) provide a policy-level perspective. Their review of Kenya's digital transformation policies revealed that while youth are active participants in the digital economy, they are not proportionally represented in cybersecurity strategies. A lack of trust in cybersecurity apps, minimal integration of cyber hygiene into education curricula, and a shortage of user-friendly tools were identified as key structural limitations. Unlike the individual-level studies, Kabaya and Kageni (2024) shift attention from users' choices to structural and policy conditions that may constrain adoption. Considered together, the Kenyan literature indicates that technology adoption is influenced by both individual protective practices and the wider educational and institutional environment.

Comparative analysis across these contexts shows a clear trend: despite high digital activity among youth and increased exposure to cyber risks, cybersecurity technology adoption remains low, both globally and regionally. Key barriers include poor user-centered design, low digital confidence, minimal institutional reinforcement, economic constraints, and misperceptions about accessibility. While global studies emphasize interface usability and personal agency, African studies highlight systemic challenges such as education gaps, localized content needs, and policy fragmentation. However, the reviewed studies differ in populations, technologies, and methodological approaches,

making it difficult to determine whether the same relationships occur among youth in a specific urban Kenyan setting.

This study builds upon these findings by investigating technology adoption behavior among youth in Westlands Constituency, Nairobi, a digitally active urban context marked by high exposure to cyber risks. Specifically, the study examined the relationship between reported technology adoption practices and mitigation of online identity theft and phishing. This localized focus addressed the limited evidence on whether protective technology practices identified in other settings are similarly associated with mitigation among youth in Westlands Constituency.

2.3.2 Cybersecurity Education

Cybersecurity education refers to structured, formal or informal efforts designed to equip individuals with the knowledge, skills, and competencies needed to identify, avoid, and respond to cyber threats, including phishing, social engineering, and identity theft (Finkelhor et al., 2021). Awareness, in contrast, emphasizes cognitive recognition of digital risks and the ability to apply preventive behaviors in real-time environments (Tick & Mai, 2021). These constructs are particularly relevant for youth populations who, while highly engaged in digital platforms, often lack foundational cybersecurity training.

Education and awareness initiatives can enhance digital hygiene, reduce susceptibility to scams, and build a culture of cyber resilience (Alkaabi et al., 2023). Effective programs focus on critical topics such as secure browsing, password management, phishing detection, multi-factor authentication, privacy settings, and ethical technology use. When

sustained and contextually relevant, these interventions may contribute to safer digital behavior and a more proactive digital mindset (Gan & Liew, 2022).

In a cross-country comparative study, Tick and Mai (2021) assessed the cybersecurity behaviors of 600 university students in Hungary and Vietnam using ANOVA and descriptive statistics. The study found alarming gaps in students' basic cyber knowledge, such as identifying phishing emails or protecting personal data. Notably, students exposed to formal cyber hygiene training demonstrated significantly more cautious digital behavior. The authors concluded that without structured cybersecurity education, digital engagement increases risk exposure, particularly among youth.

In Malaysia, Gan and Liew (2022) used Partial Least Squares Structural Equation Modeling (PLS-SEM) to assess the relationship between awareness campaigns and phishing susceptibility among 300 youth. The findings revealed that awareness training was associated with lower levels of risky behaviors, such as sharing personal data online or clicking suspicious links. The study also highlighted that information-sharing attitudes on social media were related to awareness levels, suggesting that peer culture and online behavior may be responsive to targeted interventions.

In India, Alkaabi et al. (2023) conducted a large-scale study involving over 500 university students through Likert-scale surveys and interviews. Despite high internet literacy, only 22% of students could verify the legitimacy of URLs or email headers. The researchers recommended mandatory integration of cybersecurity modules into university curricula to promote proactive defense strategies and reduce over-reliance on institutional security

systems. Taken together, Alkaabi et al. (2023), Gan and Liew (2022) and Tick and Mai (2021), agree on the importance of cybersecurity education, but their findings also indicate that general digital literacy should not be equated with cybersecurity competence. The studies differ methodologically, ranging from comparative survey analysis to PLS-SEM and mixed data collection, yet converge on the need for practical threat-recognition skills.

Ahmad et al. (2020) conducted mixed-method research in Nigeria among secondary school students. Using questionnaires and focus groups, the study uncovered that most students were aware of cybercrime in general but had not received any structured training. This gap resulted in high vulnerability to phishing, SIM swap fraud, and mobile money scams. The authors emphasized that moral education and technical training must be co-developed to influence ethical online behavior.

Riandari et al. (2024) piloted a quasi-experimental cybersecurity simulation among Indonesian teenagers using gamified phishing simulations. The pre- and post-intervention analysis revealed that participants showed substantial improvement in identifying suspicious links and avoiding deceptive messages. These findings suggest that interactive and gamified methods are effective in sustaining engagement and transferring practical skills, especially among youth. Unlike the cross-sectional Nigerian study by Ahmad et al. (2020), the quasi-experimental approach adopted by Riandari et al. (2024) provides stronger evidence regarding short-term changes following an educational intervention. However, it does not establish whether those improvements are sustained over longer periods.

In the Kenyan context, cybersecurity education is gaining attention but remains limited in both scope and impact. Sitienei (2025), in a descriptive survey of eCitizen platform users, reported that most users were unfamiliar with core protective behaviors such as enabling MFA or identifying scam messages. Their findings revealed that without formal training, even regular users of government platforms lacked essential digital protection knowledge. Mbaya and Muriuki (2023) similarly reported limited awareness and exposure to formal cybersecurity education among respondents, pointing to weaknesses in the reach of existing awareness initiatives. The Kenyan findings generally support evidence from other contexts that digital participation does not necessarily translate into cybersecurity competence. However, much of the available evidence is descriptive or cross-sectional and provides limited localized evidence on the relationship between cybersecurity education and mitigation practices among youth in Westlands Constituency**.**

Critically, most existing studies are cross-sectional and fail to assess the long-term behavioral impact of cybersecurity education. There is growing recognition of the need for longitudinal studies that can assess whether awareness leads to sustained behavior change over time. For example, measuring retention of phishing detection skills six months post-training could provide insight into intervention durability, an area still under-researched in African contexts (Alkaabi et al., 2023; Finkelhor et al., 2021).

The literature is generally consistent in indicating a positive association between cybersecurity education and safer cybersecurity behaviour, but delivery methods must be youth-centric, continuous, and practical. While global studies showcase progress through curriculum design and gamified training, Kenyan efforts remain fragmented. At the same

time, the studies differ in their measures of education, populations, and outcomes, and relatively little evidence focuses specifically on the relationship between education and mitigation of identity theft and phishing among urban Kenyan youth. This study investigated cybersecurity education among youth in Westlands Constituency and its relationship with mitigation of online identity theft and phishing, thereby addressing the identified contextual and empirical gap**.**

2.3.3 Policy Awareness

Cybersecurity policy encompasses the legal, institutional, and procedural frameworks established to deter, detect, and respond to cyber threats such as phishing, identity theft, data breaches, and digital impersonation. These frameworks serve both a preventive and corrective function, establishing enforcement protocols, outlining user rights, facilitating digital trust, and promoting inter-agency and cross-border collaboration (Mugarura & Ssali, 2021). Policy awareness concerns the extent to which individuals know and understand relevant legal and institutional protections and how they perceive their implementation. For youth, who are prolific users in the digital ecosystem, knowledge of these frameworks may shape their understanding of legal protections, reporting channels, and institutional responses to cybercrime**.**

In Kenya, cybersecurity policy has evolved through key statutes including the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and the National Cybersecurity Strategy (2022–2027). While comprehensive in scope, these instruments have faced implementation challenges. Existing literature points to limited public

awareness, dissemination, institutional enforcement, and engagement with legal protection mechanisms, particularly among digitally active populations. These limitations create a gap between the existence of cybersecurity legislation and its practical visibility to individual users.

This policy gap is not unique to Kenya. In Nigeria, Mugarura and Ssali (2021) examined the relationship between cybersecurity legislation and its practical implementation and identified a disconnect between legislation and behavior. Their analysis highlighted challenges including poor grassroots sensitization, inefficient justice systems, and perceived delays in enforcement. The study recommended localized outreach programs that communicate the relevance of legal protections in youth-friendly formats, such as digital storytelling, social media campaigns, and peer-led forums.

Globally, policy effectiveness has been shown to improve when legislation is reinforced with active awareness campaigns and community-based enforcement. In the United Kingdom, the Cyber Security Breaches Survey (2023) demonstrated the continuing importance of cybersecurity awareness alongside formal organizational policies. Similarly, in the United States, Finklea and Theohary (2020) noted that phishing continues to be a major cybercrime concern despite an established regulatory framework, suggesting a disconnect between policy development and public adoption. Collectively, these studies suggest that the existence of laws and formal policies does not automatically translate into awareness, trust, or protective action among users.

In East Africa, Mugarura and Ssali (2021) conducted a multi-country comparative review of cybersecurity legislation. Their findings highlighted a regional pattern: while many laws mirror international best practices, they often lack supporting institutional structures such as judicial training, cyber forensic capabilities, and cross-agency coordination. The result is often a fragmented enforcement landscape, where victims, especially youth, receive minimal protection or redress. The study also emphasized that the top-down nature of most cyber policies neglects participatory frameworks that could empower communities to co-own their digital safety.

At the national level, Agina (2022) assessed Kenya's policy effectiveness through judicial case analysis and found that cybercrime reporting systems are poorly structured, resulting in underreporting, particularly by youth. Although the Data Protection Act (2019) is widely regarded as a progressive statute, Agina notes that implementation has stalled due to bureaucratic bottlenecks, funding limitations, and overlap in institutional mandates. Moreover, policies have not been embedded within platforms most frequented by youth, such as mobile money apps, digital learning portals, or social media spaces.

Further policy critique is presented by Kabaya and Kageni (2024) in their national review. Their analysis of Kenya's National Cybersecurity Strategy (2022–2027) acknowledges its comprehensive vision but criticizes its limited operationalization. The absence of localized action plans, especially targeting vulnerable youth, weakens its grassroots relevance (Government of Kenya [GoK], 2022). The authors propose embedding cyber policy content within school curricula, leveraging digital influencers for awareness, and

establishing in-app reporting and policy explanation features within platforms commonly used by youth.

The national and regional studies therefore converge on the existence of an implementation and awareness gap, although they approach it from different perspectives. Mugarura and Ssali (2021) emphasize institutional capacity and regional implementation, Agina (2022) focuses on reporting and institutional mandates, while Kabaya and Kageni (2024) emphasize localization and youth-oriented communication. The convergence of these findings suggests that policy awareness should be examined not simply as knowledge of legislation but also in relation to perceptions of enforcement and confidence in institutional response.

Overall, the literature reveals that while Kenya and comparable African countries have made strides in drafting and adopting cybercrime policies, these frameworks may have limited practical value to users where awareness, accessible reporting mechanisms, and institutional trust are weak. A consistent theme across contexts is the disconnect between legislation and lived experience. Policies are often top-down, legalistic, and institutionally isolated, missing opportunities to build legitimacy through schools, digital platforms, and peer networks.

This study assessed the relationship between policy awareness and mitigation of online identity theft and phishing among youth in Westlands Constituency. It examined familiarity with cybercrime and data-protection laws, perceptions of policy enforcement, and trust in institutional response. This addressed the limited localized evidence on

whether policy awareness is associated with mitigation practices among youth in a highly digitized urban Kenyan context.

2.3.4 Online Identity Theft and Phishing

Online identity theft involves the illicit acquisition and exploitation of someone's personal information without their consent, including names, passwords, identification numbers, and banking credentials, for fraudulent or criminal purposes (Choi, 2021). Closely linked to this is phishing, a technique where attackers impersonate trusted organizations to trick individuals into disclosing confidential data through channels such as emails, SMS, fraudulent websites, or phone calls (Desolda et al., 2021). These two threats often operate in tandem, with phishing functioning as the gateway through which identity theft is perpetrated. Youth, as frequent users of digital platforms, may face increased exposure to these threats where protective knowledge and practices are inadequate. Studies have shown that online routines and risky practices can increase exposure to cyber victimization (Chan-Tin et al., 2022; Guedes et al., 2022).

The psychological and social toll of identity theft among youth is well documented. A mixed-methods study by Guedes et al. (2022) in Brazil identified financial and psychological consequences associated with cyber victimization, including distrust in digital systems. This agrees with Desolda et al. (2021), who emphasised cognitive overload, interface manipulation, and attention fatigue as key factors behind phishing success. These studies recommend innovative interventions such as simplified authentication protocols and gamified training environments to reduce user errors.

Although Guedes et al. (2022) emphasizes the consequences of victimization and Desolda et al. (2021) focuses more strongly on human factors associated with phishing susceptibility, both demonstrate that effective mitigation requires attention to user behaviour rather than reliance on technical safeguards alone.

Chan-Tin et al. (2022) similarly examined protective and vulnerable strategies associated with phishing victimization and demonstrated the relevance of user behaviour to susceptibility. Together, these global studies provide evidence that individual practices and threat-recognition capabilities are important components of phishing and identity-theft mitigation, although differences in populations and contexts limit their direct applicability to Kenyan youth.

Across the African continent, youth are increasingly being targeted through localized phishing vectors that exploit digital trust in mobile money systems and social media. In Tanzania, Mwamba and Mjema (2024) found that over 67% of surveyed mobile phone users in Kariakoo Market had encountered phishing scams, particularly via SMS and fake mobile money prompts. Victims frequently suffered financial losses but were reluctant to report incidents, fearing ridicule or lack of recourse. The study recommended mobile-friendly awareness campaigns using local languages and interactive messaging to improve digital resilience. A parallel situation was reported in Nigeria by Tolulope (2022), where undergraduate students were commonly deceived through fake scholarship offers sent via email and Instagram. Many participants could not identify phishing red flags such as inconsistent sender addresses or grammatical anomalies, further emphasizing the need for

real-time detection skills embedded in university orientation and campus-wide cyber drills.

Although both studies identify substantial exposure to phishing, they highlight different dimensions of vulnerability. Mwamba and Mjema (2024) emphasize mobile-money scams and barriers to reporting, while Tolulope (2022) draws attention to deficiencies in threat recognition. The findings therefore demonstrate that mitigation encompasses both the ability to recognize and respond to threats and the availability of appropriate reporting and support mechanisms.

Kenya mirrors these regional vulnerabilities, but with unique urban dynamics. Available Kenyan literature points to continued exposure to phishing and identity-related threats alongside gaps in protective technology use, cybersecurity knowledge, reporting, and institutional awareness. However, much of the existing evidence examines these dimensions separately rather than assessing how technological, educational, and policy factors relate jointly to mitigation among youth in a specific urban constituency.

Notably, the reviewed literature points to a range of preventive strategies that have shown potential or demonstrated benefits in different contexts. Desolda et al. (2021) and Riandari et al. (2024) advocate for gamified training that improves memory retention and engagement, especially among youth. Mwamba and Mjema (2024) emphasize the potential of mobile-first, community-driven outreach embedded in everyday digital spaces like mobile payment platforms and social media. In the Kenyan context, Kabaya and Kageni (2024) argue for integrating cybersecurity content into national school curricula

and popular apps used by youth. They also recommend creating anonymous and youth-friendly reporting channels to combat the stigma around cybercrime victimhood. The diversity of these strategies shows that there is no single universally sufficient response to phishing and identity theft; rather, technological safeguards, education, reporting mechanisms, and institutional support may need to operate together.

In summary, online identity theft and phishing are rapidly evolving cyber threats that continue to affect youth across the globe and particularly in African urban contexts. The convergence of digital inexperience, weak institutional support, and limited access to practical cybersecurity tools may increase vulnerability**.** While policy frameworks and technologies exist, the lack of localized, youth-responsive implementation mechanisms remains a critical barrier. In Kenya, these challenges are compounded by underreporting, trust deficits, and limited access to digital literacy resources**.** The reviewed studies also differ substantially in their contexts, designs, populations, and measures of mitigation, making direct generalization difficult. Furthermore, technological adoption, cybersecurity education, and policy awareness are commonly examined separately rather than as related dimensions of mitigation. The present study therefore examined their individual relationships and joint predictive contribution to the mitigation of online identity theft and phishing among youth in Westlands Constituency. The empirical findings from these dimensions subsequently informed the development of the integrated cybersecurity framework.

2.4 Knowledge Gaps

Although cybercrime research has expanded globally, notable gaps remain in understanding how youth in African urban contexts, such as Kenya's Westlands Constituency, experience and respond to phishing and online identity theft. Existing studies have largely examined populations and settings outside the specific context of urban Kenyan youth, including studies of phishing and cybersecurity behaviour in international settings (Chan-Tin et al., 2022; Desolda et al., 2021; Gan & Liew, 2022; Riandari et al., 2024). Even within Kenya, scholarly attention tends to emphasize national trends, policy issues, or particular digital platforms rather than localized behavioral responses within Westlands Constituency (Agina, 2022; Kabaya & Kageni, 2024; Sitienei, 2025). Consequently, the reviewed literature provides limited empirical evidence specifically concerning how youth aged 18–35 in Westlands Constituency mitigate online identity theft and phishing through technology adoption, cybersecurity education, and policy awareness.

Methodologically, the reviewed studies employed different methodological approaches, including cross-sectional surveys, qualitative studies, policy and legislative reviews, and quasi-experimental interventions (Agina, 2022; Gan & Liew, 2022; Riandari et al., 2024; Sitienei, 2025; Tick & Mai, 2021). For example, Tick and Mai (2021) used comparative survey analysis, Gan and Liew (2022) employed PLS-SEM, Riandari et al. (2024) adopted a quasi-experimental approach, while Agina (2022) examined cybersecurity from a policy and legal perspective. Although these methodological approaches provide useful evidence, they address different populations and dimensions of cybersecurity and

therefore do not directly establish the relationships among technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing among youth in Westlands Constituency. The present study addressed this methodological gap through a descriptive correlational research design that enabled the individual relationships and joint predictive contribution of the study variables to be examined. Qualitative responses from open-ended questionnaire items and documentary evidence supplemented the quantitative findings by providing contextual information.

Another critical gap lies in the fragmented treatment of cybercrime mitigation factors. The reviewed empirical studies generally emphasize particular dimensions of cybersecurity rather than examining the three dimensions adopted in the present study within a single analytical model. For instance, Afzal et al. (2024), Zainal (2022), and Mwamba and Mjema (2024) emphasize adoption and use of protective technologies; Tick and Mai (2021), Gan and Liew (2022), and Riandari et al. (2024) focus predominantly on cybersecurity education, awareness, or threat-recognition behaviour; while Agina (2022), Mugarura and Ssali (2021), and Kabaya and Kageni (2024) address legal, policy, and institutional dimensions. While these studies provide evidence on the respective dimensions, their separate treatment leaves limited evidence on how technology adoption, cybersecurity education, and policy awareness are individually related to mitigation and the extent to which they jointly predict mitigation of online identity theft and phishing. This study addressed that gap by examining the three dimensions within a single analytical model. The resulting empirical evidence subsequently provided the basis for developing

an integrated cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency.

Moreover, despite the existence of Kenya's legal and policy frameworks, including the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and the National Cybersecurity Strategy 2022–2027, the reviewed literature identifies continuing challenges concerning policy dissemination, institutional implementation, public awareness, reporting mechanisms, and accessibility of cybersecurity protections (Agina, 2022; Kabaya & Kageni, 2024; Mugarura & Ssali, 2021). Agina (2022), for example, draws attention to weaknesses in reporting and institutional implementation, while Kabaya and Kageni (2024) highlight challenges in translating national cybersecurity provisions into localized and youth-responsive interventions. Mugarura and Ssali (2021) similarly identify a wider regional gap between formal cybersecurity legislation and its practical implementation. These findings indicate that the existence of cybersecurity legislation does not necessarily imply that young digital users are aware of the available protections, understand them, or have confidence in their enforcement. The present study therefore examined the relationship between policy awareness and mitigation of online identity theft and phishing, with policy awareness encompassing awareness of cybercrime and data-protection laws, perceptions of policy enforcement, and trust in institutional response.

Theoretical application in the reviewed literature is also fragmented across different explanations of cybersecurity behaviour. Routine Activity Theory (RAT) (Cohen & Felson, 1979), Protection Motivation Theory (PMT) Rogers, (1975), the Health Belief

Model (Rosenstock, 1974), and Institutional Theory (DiMaggio & Powell, 1983) provide different but complementary explanations relevant to cybersecurity behaviour. The reviewed studies, however, tend to emphasize particular behavioural, technological, or institutional dimensions rather than bringing these perspectives together to interpret technology adoption, cybersecurity education, policy awareness, and mitigation within the specific context of Kenyan urban youth (Chan-Tin et al., 2022; Desolda et al., 2021; Zainal, 2022). For example, behavioural cybersecurity studies emphasize protective motivation, risk recognition, and individual responses (Desolda et al., 2021; Zainal, 2022), whereas Chan-Tin et al. (2022) demonstrates the relevance of protective and vulnerable strategies to phishing victimization. Institutional and policy-oriented literature, on the other hand, emphasizes regulatory and implementation conditions (Agina, 2022; Mugarura & Sali, 2021). In this study, RAT provided the overarching theoretical perspective by explaining cybercrime vulnerability in terms of exposure, target suitability, and capable guardianship. PMT and HBM provided complementary behavioural perspectives relevant to cybersecurity education and protective responses, while Institutional Theory provided the institutional perspective relevant to policy awareness. PMT and HBM constructs were not treated as separate independent or mediating variables in the empirical model but were used to support interpretation of the behavioural and cognitive dimensions of cybersecurity mitigation.

Lastly, while educational institutions and awareness initiatives are frequently identified as important mechanisms for strengthening cybersecurity competence, the reviewed empirical evidence shows considerable variation in the form of education examined and

the outcomes assessed (Alkaabi et al., 2023; Gan & Liew, 2022; Riandari et al., 2024; Tick & Mai, 2021). Tick and Mai (2021) associated exposure to cybersecurity training with more cautious digital behaviour, while Gan and Liew (2022) examined awareness in relation to phishing susceptibility. Riandari et al. (2024) demonstrated improvements in phishing recognition following gamified simulation, whereas Alkaabi et al. (2023) identified gaps between general digital literacy and practical cybersecurity competencies. These studies support the relevance of cybersecurity education but differ in research context, educational approach, and measures of cybersecurity behaviour. Consequently, they provide limited evidence on the relationship between cybersecurity education and the broader mitigation of online identity theft and phishing among youth in Westlands Constituency. The present study addressed this gap by examining cybersecurity education in terms of exposure to cybersecurity training and awareness, ability to identify phishing messages, and knowledge of reporting channels, and determining its relationship with mitigation of online identity theft and phishing.

Therefore, the reviewed literature demonstrates five interrelated gaps. First, there is a contextual gap because available studies have predominantly examined other national, regional, institutional, or population settings rather than youth in Westlands Constituency (Agina, 2022; Chan-Tin et al., 2022; Desolda et al., 2021; Kabaya & Kageni, 2024). Second, a methodological gap arises from differences in designs and analytical approaches, with the reviewed studies examining different aspects of cybersecurity rather than the individual relationships and joint predictive contribution of the three variables adopted in the present study (Gan & Liew, 2022; Riandari et al., 2024; Sitienei, 2025; Tick

& Mai, 2021). Third, a conceptual gap exists because technology adoption, cybersecurity education, and policy-related dimensions have largely been examined separately (Afzal et al., 2024; Agina, 2022; Mugarura & Ssali, 2021; Mwamba & Mjema, 2024; Zainal, 2022). Fourth, the reviewed Kenyan and regional literature indicates an implementation and awareness gap between formal cybersecurity frameworks and users' understanding of and engagement with those frameworks (Agina, 2022; Kabaya & Kageni, 2024; Mugarura & Ssali, 2021). Finally, differences in the theoretical perspectives applied across cybersecurity studies leave scope for a more integrated interpretation of individual protective behaviour, digital guardianship, and institutional conditions (Chan-Tin et al., 2022; Desolda et al., 2021; Zainal, 2022). By addressing these gaps, the study examined technology adoption, cybersecurity education, and policy awareness within a single analytical model and used the empirical findings to develop an integrated cybersecurity framework for mitigating online identity theft and phishing among youth in Westlands Constituency. The framework developed from the study should therefore be understood as empirically informed rather than as a framework that was independently validated across other populations or contexts.

2.5 Summary of the Reviewed Literature

This chapter has critically examined the theoretical and empirical foundations related to the mitigation of online identity theft and phishing, with a focus on youth in urban Kenyan contexts. The review was structured around the three core variables of this study, technology adoption, cybersecurity education, and policy awareness, and their relationship with the mitigation of online identity theft and phishing.

The theoretical review incorporated four key perspectives: Routine Activity Theory (RAT) Cohen & Felson, (1979), which provided the overarching theoretical perspective and contextualized cyber threats in terms of exposure, target suitability, and the absence of capable guardianship; Protection Motivation Theory (Rogers, 1975), which provided a behavioural perspective for understanding threat appraisal, self-efficacy, and protective responses; the Health Belief Model (Rosenstock, 1974), which provided a complementary perspective on perceived susceptibility, severity, and protective behaviour; and Institutional Theory (DiMaggio & Powell, 1983), which provided an institutional perspective for understanding policy awareness and institutional response. PMT and HBM constructs were used as theoretical lenses rather than as separate variables or mediators in the empirical model. Together, these theories provided complementary perspectives for interpreting the technological, educational, behavioural, and institutional dimensions relevant to mitigation of online identity theft and phishing.

Empirical findings were thematically organized across global, regional, and Kenyan contexts. In relation to technology adoption, the literature revealed that although youth frequently engage with digital systems, their use of protective technologies such as multi-factor authentication and secure browsing tools remains limited and may be constrained by usability, perceived effort, digital confidence, and contextual barriers (Afzal et al., 2024; Mwamba & Mjema, 2024; Zainal, 2022). Studies on cybersecurity education highlighted that structured training and awareness initiatives are associated with stronger threat-recognition skills and safer cybersecurity behaviour, although findings differ according to educational approach, population, and research design (Alkaabi et al., 2023;

Gan & Liew, 2022; Riandari et al., 2024; Tick & Mai, 2021). With respect to policy awareness, although Kenya has made legislative progress through frameworks such as the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019), the literature identifies continuing challenges relating to implementation, policy accessibility, reporting mechanisms, public awareness, and institutional engagement (Agina, 2022; Kabaya & Kageni, 2024; Mugarura & Ssali, 2021).

Crucially, the literature review underscores the interconnected nature of the three dimensions. Studies focusing on technology adoption demonstrate the importance of accessible and usable safeguards (Afzal et al., 2024; Zainal, 2022), while cybersecurity education studies emphasize knowledge and threat-recognition capabilities (Gan & Liew, 2022; Riandari et al., 2024). Policy-oriented research additionally demonstrates the importance of accessible legal protections and effective institutional implementation (Agina, 2022; Mugarura & Ssali, 2021). However, these streams of literature predominantly examine different dimensions of the cybersecurity problem. Consequently, the reviewed evidence provides limited understanding of the individual relationships and joint predictive contribution of technology adoption, cybersecurity education, and policy awareness to mitigation of online identity theft and phishing within one localized youth population.

Furthermore, existing studies are marked by methodological and contextual gaps. The literature encompasses cross-sectional surveys, qualitative approaches, quasi-experimental interventions, and policy or legal analyses undertaken across substantially different populations and geographical settings (Agina, 2022; Gan & Liew, 2022; Riandari

et al., 2024; Tick & Mai, 2021). Although this methodological diversity strengthens the wider cybersecurity knowledge base, it limits direct comparison and transferability to youth in Westlands Constituency. Similarly, the different theoretical emphases evident in behavioural, victimization, technology-adoption, and institutional studies indicate the value of a complementary theoretical perspective for interpreting cybersecurity mitigation (Chan-Tin et al., 2022; Desolda et al., 2021; Mugarura & Ssali, 2021; Zainal, 2022). The present study addressed this theoretical requirement by positioning RAT as the overarching theory and drawing complementary explanatory perspectives from PMT, HBM, and Institutional Theory.

In response to these gaps, this study examined the relationships between technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing and further assessed the joint predictive contribution of the three independent variables to mitigation. The findings from these analyses provided the empirical basis for developing the integrated cybersecurity framework. The insights from the reviewed literature directly informed the development of the study's conceptual framework presented in the next section. This framework visualized the hypothesized relationships between technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing and provided the structural basis for the study's methodological and analytical direction.

2.6 Conceptual Framework

A conceptual framework is an analytical structure that guides research by visually and narratively presenting the key variables and their hypothesized relationships based on theoretical and empirical foundations. Miles, Huberman, and Saldaña (2014) describe a conceptual framework as a tool presented visually or descriptively that outlines the key concepts, variables, and expected relationships among them within a study. It provides direction for data collection, interpretation, and the development of research instruments by anchoring the research problem within a theoretical context. This study's conceptual framework drew upon four interrelated theories: Routine Activity Theory (Cohen & Felson, 1979), Protection Motivation Theory (Rogers, 1975), Health Belief Model (Rosenstock, 1974), and Institutional Theory (DiMaggio & Powell, 1983). These theoretical perspectives provided complementary explanations of individual exposure to cyber threats, protective behaviour, cybersecurity awareness, and the institutional environment within which youth respond to online identity theft and phishing.

Routine Activity Theory (RAT) suggests that criminal acts occur when a motivated offender comes into contact with a suitable target in the absence of effective guardianship (Cohen & Felson, 1979). In the digital context, frequent online engagement may increase opportunities for exposure to phishing and identity-related threats. Protection Motivation Theory (PMT) explains protective behaviour through individuals' appraisal of threats and their ability to undertake appropriate protective responses (Rogers, 1975). In this study, PMT provided a basis for understanding cybersecurity awareness, confidence in avoiding cyber threats, and engagement in protective digital practices.

The Health Belief Model (HBM) incorporates behavioural and cognitive components, particularly perceived susceptibility, severity, and self-efficacy, which are relevant to understanding how individuals perceive cyber risks and respond to them (Du et al., 2024). Institutional Theory contributed to understanding how formal structures, legal frameworks, enforcement mechanisms, and institutional trust shape awareness and perceptions of cybersecurity policies and reporting mechanisms (Delso-Vicente et al., 2025). Together, these theoretical perspectives provided a basis for examining the technological, educational, behavioural, and institutional dimensions captured in the study.

The conceptual framework proposed in this study brings together three independent variables-technology adoption, cybersecurity education, and policy awareness-and their relationship with the mitigation of online identity theft and phishing, which served as the dependent variable. Technology adoption captured the use of digital security tools and protective practices. Cybersecurity education encompassed training and awareness, the ability to recognize phishing attempts, and knowledge of appropriate reporting channels. Policy awareness captured respondents' awareness and understanding of cybercrime and data-protection laws, perceptions of policy enforcement, and trust in institutional responsiveness.

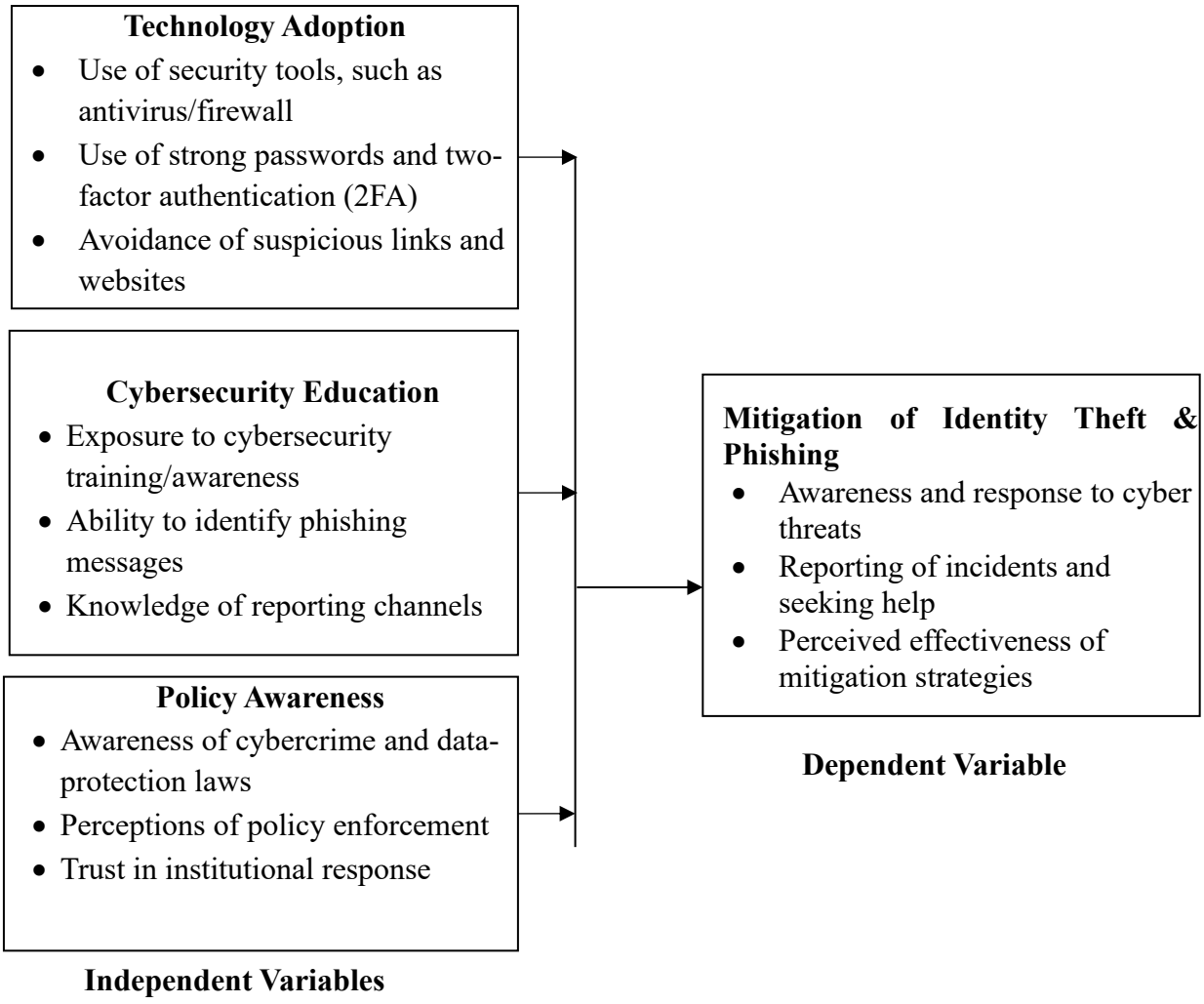
The dependent variable, mitigation of identity theft and phishing, captured behavioural and cognitive dimensions. These included awareness and response to cyber threats, reporting of incidents and seeking appropriate assistance, and perceptions of the effectiveness of different mitigation strategies. The dependent variable was therefore

treated as a multidimensional outcome reflecting how youth understand, respond to, and perceive measures for addressing online identity theft and phishing.

The hypothesized relationships indicate that technology adoption, cybersecurity education, and policy awareness are individually related to the mitigation of online identity theft and phishing and jointly predict the dependent variable. The empirical assessment of these relationships provided the basis for integrating the technological, educational, and policy dimensions into the integrated cybersecurity framework developed based on the empirical findings of the study. Figure 2.1 presents the conceptual framework.

Figure 2. 1:

Conceptual Framework



CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research methodology adopted to examine the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County. Methodological rigour is important for ensuring the validity, reliability, and credibility of the study findings (Creswell & Creswell, 2018). The methodology was guided by the study objectives and conceptual framework and provided a systematic basis for data collection, analysis, interpretation, and development of the proposed empirically informed cybersecurity framework.

The chapter is organized into ten sections. Section 3.2 presents the research design, while Section 3.3 describes the target population. Section 3.4 explains the sampling technique and sample size determination. Section 3.5 presents the data collection instruments, comprising the semi-structured questionnaire and document review guide. Section 3.6 describes the data collection procedures, while Section 3.7 presents the pilot study. Section 3.8 discusses the validity and reliability of the research instruments. Section 3.9 presents the data analysis techniques and procedures for presentation of the findings, including the procedure used to develop the proposed cybersecurity framework. Section 3.10 outlines the ethical considerations observed throughout the study.

3.2 Research Design

A research design functions as a strategic framework that guides how data is gathered, measured, and interpreted in accordance with the study's aims and underlying philosophical stance (Creswell & Creswell, 2018). This study employed a descriptive correlational research design with qualitative supplementation, which was appropriate for examining statistical associations among existing variables, specifically technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing, without introducing any experimental intervention or altering the natural setting (Fraenkel et al., 2019). This design was particularly appropriate for the research questions, which sought to determine the individual relationships between the independent variables and mitigation of online identity theft and phishing and their joint predictive contribution, rather than establishing causality. Such relationship-focused questions are best addressed through correlational methods, which are widely used in behavioral and social science research where random assignment and experimental control are impractical (Gay et al., 2012; McMillan & Schumacher, 2014).

The descriptive component allowed the researcher to characterize the digital practices and cybersecurity awareness levels of urban youth, while the correlational aspect enabled examination of the statistical relationships between the study variables in their natural setting. The study was predominantly quantitative, with qualitative responses from the open-ended questionnaire items used to supplement the quantitative findings. Document review provided additional contextual information on relevant cybersecurity policies and institutional mechanisms. In summary, the descriptive correlational research design with

qualitative supplementation provided an efficient, ethically sound, and statistically appropriate method for examining the study relationships and generating empirical evidence that informed the development of the integrated cybersecurity framework for youth within Westlands Constituency.

3.3 Target Population

The target population refers to the entire group of individuals possessing characteristics relevant to a study and from whom information may be obtained to address the research objectives (Mugenda & Mugenda, 2003). In this study, the target population comprised youth aged 18–35 years residing in Westlands Constituency, Nairobi County. This population was selected because of its active engagement with digital technologies and exposure to cyber risks such as online identity theft and phishing.

According to the 2019 Kenya Population and Housing Census, Westlands had a total population of 308,854 residents (KNBS, 2019). The study, however, specifically targeted residents aged 18–35 years. Based on the age distribution reported in the KNBS 2019 Census Volume III, the population comprised 4,074 persons aged 18 years, 5,115 aged 19 years, 33,981 aged 20–24 years, 34,987 aged 25–29 years, 32,197 aged 30–34 years, and 6,444 aged 35 years. The target population for the study was therefore 116,798 youth aged 18–35 years. KNBS Volume III reports population by single-year and five-year age groups at sub-county level, providing the basis for determining this target population.

Westlands is characterized by a diverse urban population comprising university students, young professionals, and youth engaged in formal and informal economic activities. This

diversity provided an appropriate setting for examining differences in technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing. The study therefore focused on eligible youth aged 18–35 years residing in Westlands Constituency as the population relevant to the study objectives.

3.4 Sampling Technique and Sample Size

3.4.1 Sampling Technique

Sampling involves drawing a representative portion of individuals from a larger target population to obtain information relevant to the objectives of a study (Kothari, 2004). This research employed purposive sampling to select participants who satisfied predetermined eligibility requirements. The eligibility criteria required participants to: (i) be aged between 18 and 35 years; (ii) have resided in Westlands Constituency for at least one year; (iii) possess basic digital literacy; and (iv) have regular access to an internet-enabled device. These criteria ensured that participants belonged to the population relevant to the study and had sufficient exposure to digital environments in which online identity theft and phishing may occur.

Purposive sampling was appropriate because the study focused on a specific category of youth defined by age, residence, digital literacy, and access to internet-enabled devices. Eligible participants were drawn from diverse socio-economic and occupational backgrounds within Westlands Constituency, including university students, young professionals, youth engaged in the informal sector, and residents from different neighbourhoods, including Kangemi and Githogoro. This approach enabled the study to

capture participants with varying levels of education, income, device access, and digital exposure, which were relevant to understanding differences in cybersecurity practices and experiences.

Participant recruitment was undertaken through targeted outreach within Westlands Constituency. The questionnaire was distributed through digital platforms commonly used by the target population, including WhatsApp, Telegram, Facebook, and email, alongside outreach through youth groups, community centres, and local vocational institutions. Screening questions embedded in the questionnaire were used to establish whether prospective participants met the inclusion criteria before their responses were included in the study. This recruitment approach was particularly appropriate because a comprehensive sampling frame containing the names and contact details of all eligible youth aged 18–35 years in Westlands Constituency was not available.

To enhance the diversity of the respondents reached through purposive sampling, recruitment targeted youth from different educational, occupational, socio-economic, and digital-access backgrounds. Information on characteristics such as education level and digital engagement was also collected to facilitate interpretation of variations within the study population. The sampling procedure therefore ensured that participation was restricted to respondents who met the study's eligibility criteria while providing access to youth with diverse experiences of technology use, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing.

3.4.2 Sample Size Determination

The sample size for this study was calculated using Yamane's (1967) formula, which is commonly used to determine an appropriate sample size from a known finite population. The formula was expressed as:

$$n = \frac{N}{(1 + N(e)^2)}$$

Where:

n = the required sample size

N = the total population size (116,798 youth)

e = the acceptable margin of error (set at 0.05 for 95% confidence level)

Based on the 2019 Kenya Population and Housing Census, the target population comprised 116,798 youth aged 18–35 years in Westlands Constituency (KNBS, 2019). Therefore:

$$n = \frac{116{,}798}{(1+116{,}798 * 0.05^2)} = \frac{116{,}798}{292.995} \approx 398.64$$

n=398.64 ≈399

The final sample size was therefore 399 respondents. This sample size was considered adequate for the correlational and regression analyses undertaken in the study and provided sufficient observations for examining relationships among the study variables (Creswell & Creswell, 2018). Contextually, the sample size was appropriate given the socio-economic and digital diversity of youth in Westlands Constituency and enabled the

study to capture respondents with varying educational backgrounds, digital engagement patterns, and access to cybersecurity tools. The open-ended questionnaire items provided supplementary qualitative information from the respondents, consistent with the descriptive correlational research design with qualitative supplementation.

3.5 Data Collection Instruments

The research utilized two data collection instruments: a semi-structured questionnaire and a document review guide. The semi-structured questionnaire served as the principal instrument for collecting quantitative data, while its open-ended items provided supplementary qualitative information. The document review guide was used to obtain contextual information from relevant cybersecurity policies, reports, and institutional documents. The instruments were aligned with the study's conceptual framework, which examined the relationships between technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing among youth in Westlands Constituency.

3.5.1 Semi-Structured Questionnaire

The semi-structured questionnaire served as the core tool for collecting primary data from youth in Westlands Constituency aged 18 to 35 years. The questionnaire was designed to capture both numerical patterns and explanatory insights. Closed-ended questions, primarily using Likert scales, collected quantifiable data on respondents' behavior, attitudes, and knowledge levels regarding cybersecurity tools, education exposure, and awareness of digital policy frameworks. Open-ended items allowed participants to share

personal experiences, opinions, or challenges faced in practicing digital safety, thus adding depth and nuance to the numerical data.

The development of the questionnaire was informed by Routine Activity Theory (RAT) (Cohen & Felson, 1979), Protection Motivation Theory (PMT; Rogers, 1975), the Health Belief Model (HBM; Rosenstock, 1974), and Institutional Theory (DiMaggio & Powell, 1983). RAT provided the overarching theoretical perspective, while PMT and HBM provided complementary behavioural perspectives and Institutional Theory provided the institutional perspective relevant to policy awareness. These theoretical perspectives informed the development and interpretation of questionnaire items relating to technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing.

The questionnaire underwent pretesting through a pilot study with 40 participants drawn from Dagoretti North, a demographically similar constituency to Westlands. This pretest assessed the clarity, relevance, and internal consistency of questionnaire items. The internal reliability of the scales was measured using Cronbach's alpha, with a threshold of 0.70 (Nunnally & Bernstein, 1994). Additionally, content validity was ensured through reviews by two academic experts in cybersecurity and one practitioner familiar with youth digital behavior. Their feedback was used to revise ambiguous or redundant items.

For logistical and ethical efficiency, the questionnaire was administered online using Google Forms. This mode was appropriate given the study's digitally literate target population and supported respondent anonymity while reducing interviewer influence.

Online delivery also allowed the researcher to reach participants across different neighborhoods in Westlands while minimizing disruptions to their schedules. However, recognizing that exclusive reliance on online platforms such as Gmail, WhatsApp, or Facebook could bias participation toward more digitally active or higher-income youth, the researcher supplemented online distribution with targeted outreach through youth groups, community centres, and local vocational institutions to reach participants with varying levels of digital access and socio-economic backgrounds.

3.5.2 Document Review Guide

The second instrument, a structured document review guide, facilitated the systematic examination of relevant secondary data. This included policy texts such as the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), the National Cybersecurity Strategy (2022–2027), crime statistics from the National Crime Research Centre (NCRC), and police records where accessible. To enhance clarity and analytical depth, the document review also included: Annual reports from the Communications Authority of Kenya (CAK), Cybersecurity advisories and alerts issued by KE-CIRT/CC, Court cases and judgments involving cybercrime incidents affecting youth, NGO or civil society reports focused on digital literacy and youth online safety, and Peer-reviewed studies documenting cybercrime patterns in urban Kenya.

The review guide focused on thematic categories such as policy implementation mechanisms, youth-specific outreach strategies, institutional enforcement trends, and documented cybercrime patterns. Document analysis provided contextual information that

supplemented the interpretation of findings obtained from the questionnaire. Relevant information extracted from the documents was organized according to the study variables and used to provide additional context on cybersecurity policies, institutional mechanisms, and documented cybercrime trends.

3.6 Data Collection Procedures

Data collection procedures involved the organized sequence of activities undertaken by the researcher to obtain relevant information systematically for addressing the study objectives (Creswell & Creswell, 2018). In this study, data were gathered from primary and secondary sources using a semi-structured questionnaire and a document review guide. The questionnaire served as the principal instrument for collecting quantitative data, with open-ended items providing supplementary qualitative information, while document review provided contextual information relevant to the interpretation of the study findings.

The primary data collection process began with obtaining formal authorization from the relevant bodies. Ethical approval was obtained from the Kenya Methodist University Research Ethics Committee, after which a research permit was secured from the National Commission for Science, Technology and Innovation (NACOSTI). Additionally, letters of introduction were obtained from local administrative offices within Westlands Constituency to facilitate community access during data collection.

After obtaining the required approvals, the researcher purposively identified youth aged 18 to 35 years who met the inclusion criteria: residency in Westlands Constituency for at

least one year, access to an internet-enabled device, and basic digital literacy. A link to the semi-structured questionnaire was shared through digital platforms such as WhatsApp, Telegram, Facebook, and email. Targeted outreach through youth groups, community centres, and local vocational institutions was also used to reach eligible participants from different socio-economic and digital-access backgrounds. Screening questions embedded in the questionnaire were used to confirm participants' eligibility. The potential for online recruitment to favour more digitally active participants was acknowledged and considered when interpreting the findings.

Informed consent was obtained through an introductory section embedded in the online questionnaire. This section clearly outlined the purpose of the study, participants' rights, voluntary participation, and assurance of confidentiality. Respondents were required to confirm their consent by ticking a checkbox before accessing the rest of the questionnaire. To improve response rates, two follow-up reminders were sent at intervals of three to five days using the same online platforms, encouraging participation without exerting pressure.

Secondary data were collected through a structured document review process. The review covered relevant cybersecurity legislation, policies, reports, and institutional documents, including the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), the National Cybersecurity Strategy (2022–2027), and relevant cybercrime reports and advisories. The document review focused on policy implementation, cybersecurity awareness initiatives, reported cybercrime trends, and institutional responses relevant to

online identity theft and phishing. The documentary evidence was used to provide contextual information that supplemented interpretation of the questionnaire findings.

All collected data were securely managed. Responses from the online survey were stored in password-protected electronic storage with appropriate access controls, while document review materials and field notes were stored in password-protected folders accessible only to the researcher and authorized personnel. These procedures safeguarded participant confidentiality and supported the secure management of data throughout the study.

3.7 Pilot Study

A pilot study serves as an initial trial to assess the clarity, dependability, and practical functionality of research tools prior to the main data collection phase (Mugenda & Mugenda, 2003). In this research, the pilot involved 40 participants, representing 10% of the total sample selected from youth residing in Dagoretti North Sub-County, a region with similar demographic characteristics to Westlands. This group was excluded from the final sample to avoid bias. The main objectives of the pilot were to: (i) assess the clarity and logical flow of questionnaire items, (ii) evaluate the internal reliability of scales, and (iii) test the usability of the online data collection tool. Feedback was gathered through an embedded comment section within the questionnaire and follow-up calls with a few participants. Responses were reviewed for item ambiguity, dropout patterns, and reliability scores (e.g., Cronbach's alpha). Findings from the pilot informed revisions to

improve item wording, sequencing, and functionality, ensuring that the final instrument is valid, reliable, and contextually appropriate for the target population.

3.8 Validity and Reliability of Research Instruments

This section described how both the validity and the reliability were established and maintained throughout the study (Creswell & Creswell, 2018) which is essential for producing accurate, consistent, and credible results.

3.8.1 Validity

Validity denotes how well a research instrument captures the specific concepts or constructs it is designed to measure (Creswell & Creswell, 2018). This study evaluated content validity and construct validity. Content validity was ensured through consultation with subject matter experts who assessed the relevance and adequacy of the instrument's items. The draft questionnaire was evaluated by two university research supervisors and one practicing cybersecurity expert. These reviewers assessed whether each item is relevant, clear, and comprehensive in addressing the intended variables. Their ratings were analyzed using the Content Validity Index (CVI), where an item-level CVI score of 0.78 or above was considered acceptable (Polit & Beck, 2006).

Construct validity was assessed during the pilot study phase, where participant responses were examined to determine whether they logically group under their respective constructs such as technology adoption, cybersecurity education, and policy awareness. Ambiguities or inconsistencies in how items relate to their underlying variables was identified and corrected.

The validity assessment was further supported by contextual triangulation with document review findings. Documentary information from relevant government and institutional sources was used to provide contextual comparison with questionnaire findings. This supplementary comparison enhanced the contextual interpretation of the study findings but was not treated as a separate statistical test of validity.

3.8.2 Reliability

Reliability refers to the degree to which a measurement instrument consistently yields similar results under comparable conditions (Fraenkel et al, 2019). This study employed Cronbach's alpha as the principal indicator for evaluating the internal consistency of items within each construct. A benchmark score of 0.70 or above was considered the minimum acceptable level of reliability, in line with established norms in social science research (Mugenda & Mugenda, 2003; Nunnally & Bernstein, 1994). The reliability analysis was performed using data obtained from the pilot sample of 40 respondents. Each construct was assessed independently. Cronbach's alpha was used to determine the internal consistency of the questionnaire items, with a coefficient of 0.70 or above considered acceptable. Items identified during the pilot study as unclear or inconsistent with their respective constructs were reviewed before the questionnaire was finalized for the main study.

3.9 Data Analysis Techniques and Presentation

Data analysis involves systematically organizing, refining, interpreting, and presenting research data to effectively address the study's objectives and research questions (Creswell

& Creswell, 2018). In this study, quantitative data from the closed-ended questionnaire items formed the principal basis of analysis, while qualitative information from open-ended questionnaire items and document review supplemented the interpretation of the quantitative findings. Statistical techniques were used to analyze the quantitative data, while thematic analysis was applied to the supplementary qualitative information.

3.9.1 Quantitative Data Analysis

Quantitative data analysis entails the systematic arrangement, interpretation, and statistical examination of numerical data to address the research questions of the study (Creswell & Creswell, 2018). Quantitative data were obtained from the closed-ended sections of the semi-structured questionnaire and analyzed using SPSS Version 29. The analysis began with data cleaning, which included checking for missing values, detecting outliers, and eliminating incomplete or inconsistent entries. Descriptive statistics such as frequencies, percentages, means, and standard deviations were then used to summarize respondent demographics and key patterns related to technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing.

To assess the assumptions underlying parametric analysis, tests for normality, homoscedasticity, and multicollinearity using Variance Inflation Factors were conducted. These checks supported the appropriateness of the subsequent inferential procedures. Pearson's correlation coefficient was employed to assess the strength and direction of the relationships between the independent variables and the dependent variable. Simple linear

regression analysis was also conducted to examine the predictive relationship between each independent variable-technology adoption, cybersecurity education, and policy awareness-and mitigation of online identity theft and phishing. Multiple linear regression analysis was subsequently conducted to determine the joint predictive contribution of technology adoption, cybersecurity education, and policy awareness to mitigation of online identity theft and phishing, thereby addressing the fourth specific objective. Statistical significance was determined at the 0.05 alpha level. This structured approach allowed the study to test associations and predictive relationships without implying causality. The findings further provided empirical evidence for the development of the proposed integrated cybersecurity framework.

3.9.2 Qualitative Data Analysis

Qualitative data were obtained from two sources: open-ended responses embedded in the questionnaire and secondary information obtained through document review. The qualitative data were examined using thematic analysis to identify, interpret, and present recurring patterns and themes within the textual information (Braun & Clarke, 2006).

Open-ended responses from participants were organized and coded to identify recurring ideas related to the study objectives. The identified codes were grouped into broader themes and interpreted alongside the quantitative findings to provide supplementary explanations and contextual insights.

Document analysis was conducted on the cybersecurity legislation, policies, reports, and institutional documents identified for review. Using the structured document review guide,

relevant information was extracted and organized according to themes relating to cybersecurity policy implementation, awareness, institutional responses, and mitigation of online identity theft and phishing.

The qualitative findings were used to supplement and contextualize the quantitative findings rather than as a separate analytical strand. This provided additional insight into the experiences, challenges, and institutional context surrounding cybersecurity mitigation among youth in Westlands Constituency.

3.9.3 Cybersecurity Framework Development Procedure

The integrated cybersecurity framework was developed based on the empirical findings of the study and the theoretical and empirical literature reviewed. The development process involved synthesizing findings relating to technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing. Descriptive findings were used to identify prevailing cybersecurity practices and gaps among the respondents, while correlation analysis established the individual relationships between the three independent variables and mitigation. Multiple regression analysis was used to determine their joint predictive contribution and the relative contribution of each predictor to mitigation.

The quantitative findings were supplemented by responses from the open-ended questionnaire items and relevant information obtained through document review. These findings were interpreted alongside Routine Activity Theory as the overarching theoretical perspective, with Protection Motivation Theory, the Health Belief Model, and Institutional

Theory providing complementary perspectives. The resulting evidence was organized around the technological, educational, and policy dimensions and integrated to establish the key components and relationships represented in the proposed cybersecurity framework.

The framework therefore represented an empirically informed integration of the study findings rather than a separately validated model. Its development focused on translating the relationships identified in the study into a structured framework for mitigating online identity theft and phishing among youth in Westlands Constituency. Independent external validation or field testing of the developed framework was beyond the scope of the study.

3.9.4 Data Presentation

Findings from the data analysis were presented through tables, graphical illustrations, and descriptive narratives. Visual representations such as bar charts, pie diagrams, and frequency tables were employed to summarize descriptive statistics, with the choice of format tailored to the nature and measurement level of each variable to enhance interpretability. Inferential results, such as correlations and regression outputs, were presented using summary tables with associated significance levels.

Qualitative findings from open-ended responses and document review were used to supplement the presentation and interpretation of the quantitative findings. Relevant thematic summaries and documentary evidence were incorporated where appropriate to provide additional context to the statistical findings. This approach supported a clearer interpretation of the findings in relation to the study objectives and informed the

conclusions, recommendations, and development of the proposed integrated cybersecurity framework.

3.10 Ethical Considerations

This study recognized that ethical compliance is paramount, especially when dealing with potentially sensitive issues such as identity theft and phishing among youth. It adheres to the ethical protocols established by the Kenya Methodist University (KeMU) Ethics Review Committee and the National Commission for Science, Technology and Innovation (NACOSTI), as well as international research ethics guidelines outlined in the Belmont Report and the Declaration of Helsinki (Resnik, 2020; WHO, 2011). Prior to data collection, the researcher obtained formal ethical clearance from KeMU and a research permit from NACOSTI. Letters of introduction from sub-county administrators and chiefs within Westlands Constituency were secured to enhance transparency and ensure community-level access. These documents also supported researcher legitimacy and foster trust with participants.

Prior to participation, all individuals were required to give informed consent. The online questionnaire begun with a consent form that clearly explains the study's objectives, procedures, potential risks and benefits, measures for confidentiality, and emphasizes the voluntary nature of participation. Participants confirmed their consent by ticking an "I Agree" box, which grants them access to the rest of the questionnaire. This process ensures transparency and digitally documents consent in a secure manner.

To maintain confidentiality and protect participant anonymity, no personal identifiers were collected. Each respondent was assigned a unique, anonymous code for data tracking. All survey responses were stored in encrypted, password-protected cloud storage Google Drive, with access restricted through two-factor authentication. Backup copies were maintained on encrypted external storage devices, accessible only by the researcher and authorized supervisors. In compliance with the British Psychological Society's data protection guidelines (2014), all raw data was retained for a period of six months after the study concludes and was then permanently deleted.

To minimize psychological harm, the questionnaire was designed to avoid triggering or intrusive content. Participants were not asked to recount specific victimization incidents unless they choose to do so voluntarily in open-ended items. Additionally, the researcher provided a list of mental health resources and counseling contacts in the debriefing section of the survey to support any participant who may feel discomfort during the process. Continuous ethical monitoring was integrated into the research process. Any protocol amendments during the data collection phase was reported to KeMU's Ethics Review Committee for approval. Updates were also communicated to NACOSTI as necessary. These procedures reflected the researcher's commitment to maintaining ethical rigor and respect for participant rights throughout the study cycle.

CHAPTER FOUR: RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the analysis and interpretation of data on the relationships between technology adoption, cybersecurity education, policy awareness, and perceived effectiveness of mitigation strategies against online identity theft and phishing among youth in Westlands Constituency. Descriptive statistics, correlation analysis, and regression analysis were used to address the quantitative research objectives. Qualitative findings from the open-ended questionnaire items and document review were used to supplement the interpretation of the quantitative findings. The chapter first presents the response rate and demographic characteristics, followed by measurement quality and operationalization of the study variables, results relating to each research objective, the proposed empirically informed cybersecurity framework, and discussion of the findings.

4.2 Response Rate

The study targeted a sample of 399 respondents drawn from youth aged 18 to 35 years in Westlands Constituency, Nairobi County, as specified in the study design. Out of the 399 questionnaires administered, 338 were duly completed and returned, while 61 were not returned or were incomplete. This yielded a response rate of 84.7%, as presented in Table 4.1. The achieved response rate of 84.7% is considered high and adequate for statistical analysis. According to Mugenda and Mugenda (2003), a response rate of 50% is adequate, 60% is good, and 70% and above is regarded as very good. Therefore, the response rate

obtained in this study falls within the “very good” category, indicating a high level of respondent participation.

Table 4.1

Response Rate

Category	Frequency	Percentage (%)
Questionnaires Distributed	399	100.0
Questionnaires Returned	338	84.7
Non-response	61	15.3
Total	399	**100.0**

4.3 Pilot Test Results

A pilot study was conducted before the main data collection to assess the validity and reliability of the research instrument. The pilot study involved 40 respondents who possessed characteristics similar to those of the target population but were not included in the main study. The assessment focused on the validity of the questionnaire items and the internal consistency of the constructs measured in the study. The findings of the pilot test are presented in the following subsections.

4.3.1 Validity of the Research Instrument

Validity was assessed to establish whether the questionnaire items adequately measured the constructs they were intended to measure. Content validity was assessed through expert review involving two university research supervisors and one practising cybersecurity expert. The experts evaluated the questionnaire items for relevance, clarity, and adequacy in measuring the study variables. The Content Validity Index (CVI) was

computed from the expert ratings. An item-level CVI of 0.78 or above was considered acceptable. The results are presented in Table 4.2.

Table 4.2

Content Validity Results

Construct	Number of Items Assessed	CVI	Decision
Technology Adoption	6	0.89	Valid
Cybersecurity Education	5	0.87	Valid
Policy Awareness	5	0.84	Valid
Mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies)	5	0.86	Valid
Overall Instrument	**21**	**0.87**	**Valid**

The results indicate that the CVI values for all the constructs were above the minimum acceptable threshold of 0.78. Technology adoption recorded a CVI of 0.89, cybersecurity education 0.87, policy awareness 0.84, and mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies) 0.86. The overall instrument recorded a CVI of 0.87, indicating that the questionnaire items were considered relevant and adequate for measuring the study constructs.

Construct validity was further assessed during the pilot study by examining whether the questionnaire items corresponded logically with their respective constructs. Items relating to technology adoption, cybersecurity education, policy awareness, and mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies) were reviewed for conceptual consistency. Items identified as unclear or ambiguous during the pilot exercise were refined before administration of the final questionnaire.

4.3.2 Reliability of the Research Instrument

Reliability analysis was conducted using responses obtained from the 40 pilot respondents. Cronbach's alpha was used to assess the internal consistency of the items measuring each study construct. In accordance with the criterion specified in Chapter Three, a Cronbach's alpha coefficient of 0.70 or above was considered acceptable. The findings are presented in Table 4.3.

Table 4.3

Reliability Test Results

Construct	Number of Items	Cronbach's Alpha	Decision
Technology Adoption	6	0.84	Reliable
Cybersecurity Education	5	0.86	Reliable
Policy Awareness	5	0.79	Reliable
Mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies)	5	0.81	Reliable
Overall Instrument	**21**	**0.85**	**Reliable**

The results show that all the study constructs attained Cronbach's alpha coefficients above the minimum acceptable threshold of 0.70. Cybersecurity education recorded the highest reliability coefficient ($\alpha = 0.86$), followed by technology adoption ($\alpha = 0.84$), mitigation of identity theft and phishing (perceived effectiveness of mitigation strategies) ($\alpha = 0.81$), and policy awareness ($\alpha = 0.79$). The overall instrument recorded a Cronbach's alpha coefficient of 0.85, demonstrating satisfactory internal consistency.

The pilot results therefore indicated that the questionnaire had acceptable validity and reliability for use in the main study. Following the pilot exercise, items requiring

clarification were reviewed before the final questionnaire was administered to respondents in Westlands Constituency.

4.4 Demographic Characteristics of Respondents

This section presents the demographic profile of the respondents, including age, gender, level of education, employment status, duration of residence in Westlands Constituency, and patterns of internet use. These characteristics provide important contextual insights for interpreting the study findings on cybersecurity behavior among youth.

Table 4.4

Demographic Characteristics of Respondents

Variable	Category	Frequency	Percentage (%)
Age (Years)	18–22	96	28.4
	23–27	104	30.8
	28–31	72	21.3
	32–35	66	19.5
Gender	Male	178	52.7
	Female	148	43.8
	Other/Prefer not to say	12	3.5
Education Level	Secondary	58	17.2
	Tertiary (College/TVET)	96	28.4
	Undergraduate	132	39.1
	Postgraduate	52	15.4
Employment Status	Employed	96	28.4
	Self-employed	84	24.9
	Unemployed	58	17.2
	Student	100	29.6
Duration in Westlands	1–3 years	154	45.6
	Over 3 years	184	54.4
Internet Use (Daily)	Social media, learning, work, mobile services	338	100.0

The findings indicate that the majority of respondents (59.2%) were aged between 18 and 27 years, confirming that the study largely captured a youthful and highly digitally active

population. In terms of gender distribution, the sample was relatively balanced, with a slight majority of male respondents (52.7%) compared to female respondents (43.8%).

The education profile shows that a large proportion of respondents had attained tertiary and undergraduate levels of education (67.5%), indicating a relatively high level of general literacy and potential digital familiarity. Regarding employment status, respondents were distributed across students (29.6%), employed (28.4%), self-employed (24.9%), and unemployed (17.2%), reflecting diverse socio-economic backgrounds.

The duration of residence shows that all respondents had lived in Westlands Constituency for at least one year, with 54.4% residing in the area for over three years and 45.6% for between one and three years. This indicates that the respondents met the residence eligibility criterion specified for the study and had sufficient familiarity with the study area. Finally, all respondents reported daily use of the internet for activities such as social media, online learning, work, mobile banking, and e-commerce.

Overall, the demographic characteristics reflect a young, digitally active, and moderately educated population with diverse economic backgrounds. These characteristics provide contextual information for understanding the subsequent findings on technology adoption, cybersecurity education, policy awareness, and perceived effectiveness of mitigation strategies against online identity theft and phishing.

4.4.1 Descriptive Statistics on Mitigation of Identity Theft & Phishing

The dependent variable of the study was Mitigation of Identity Theft & Phishing. It was assessed using five strategies contained in Section E of the questionnaire: cybersecurity training and education programs, use of secure tools such as two-factor authentication (2FA), antivirus and spam filters, legal penalties and cybercrime enforcement, community-based awareness campaigns, and improvement of platform security by technology companies. Respondents rated the perceived effectiveness of each strategy in reducing phishing and identity theft among youth using a five-point scale, where 1 = Not Effective, 2 = Slightly Effective, 3 = Neutral, 4 = Effective, and 5 = Very Effective.

The five items were analysed individually using means and standard deviations and were also combined to obtain a composite measure of Mitigation of Identity Theft & Phishing for subsequent analysis. Higher scores represented greater perceived effectiveness of the mitigation strategies.

Table 4. 1

Perceived Effectiveness of Mitigation Strategies (n = 338)

Strategy	**Mean**	**Std. Dev**
Cybersecurity training and education programs	4.218	0.831
Use of secure tools (2FA, antivirus, spam filters)	4.074	0.874
Legal penalties and cybercrime enforcement	3.486	1.021
Community-based awareness campaigns	3.912	0.943
Tech companies improving platform security	4.103	0.886
Composite Mean	3.959	0.911

The findings indicate that respondents generally perceived the strategies assessed as effective in mitigating online identity theft and phishing, as reflected by the composite mean of 3.959 (SD = 0.911). Cybersecurity training and education programs recorded the

highest mean (M = 4.218, SD = 0.831), indicating that respondents perceived education and training as the most effective strategy. This was followed by improvement of platform security by technology companies (M = 4.103, SD = 0.886) and the use of secure tools such as two-factor authentication, antivirus software and spam filters (M = 4.074, SD = 0.874).

Community-based awareness campaigns also recorded a relatively high mean (M = 3.912, SD = 0.943). Legal penalties and cybercrime enforcement recorded the lowest mean (M = 3.486, SD = 1.021), although the score remained above the midpoint of the scale. The comparatively higher standard deviation for this strategy indicates greater variation in respondents' perceptions of the effectiveness of legal and enforcement measures.

Overall, the findings indicate favourable perceptions of the effectiveness of the five strategies in mitigating online identity theft and phishing among youth. The composite measure was subsequently used as the dependent variable in examining its relationships with technology adoption, cybersecurity education and policy awareness.

4.5 Technology Adoption and Mitigation of Online Identity Theft and Phishing

This section examines the extent to which technology adoption is associated with the mitigation of online identity theft and phishing among youth in Westlands Constituency. Technology adoption in this study refers to the use of digital security practices and tools such as multi-factor authentication, strong password management, secure browsing, and the ability to detect phishing attempts.

This analysis is guided by the research objective: to assess the extent of technological adoption in mitigating online identity theft and phishing among youth in Westlands Constituency, Nairobi County, and the corresponding research question: what relationship exists between technology adoption and mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County?

The analysis is structured to provide a comprehensive assessment of this relationship. It begins with descriptive statistics to establish the level of adoption of cybersecurity technologies among respondents, followed by correlation analysis to determine the strength and direction of the relationship between technology adoption and mitigation. Regression analysis is then conducted to evaluate the extent to which technology adoption predicts mitigation outcomes. In addition, qualitative insights are integrated to explain user experiences, highlight barriers to adoption, and provide deeper understanding of behavioral patterns influencing the use of cybersecurity measures.

4.5.1 Descriptive Analysis of Technology Adoption

This section presents descriptive statistics on the level of technology adoption among respondents, focusing on key cybersecurity practices including the use of multi-factor authentication (MFA), password management practices, secure browsing behavior, and the ability to detect phishing attempts. A five-point Likert scale was used to measure responses, where 1.000–1.800 = Strongly Disagree, 1.801–2.600 = Disagree, 2.601–3.400 = Neutral/Moderate, 3.401–4.200 = Agree, and 4.201–5.000 = Strongly Agree. Table 4.7 presents summary of findings obtained.

Table 4. 2:

Descriptive Statistics for Technology Adoption

Statement	Mean	Std. Dev
I regularly use antivirus software or firewalls	3.462	0.988
I use strong, unique passwords for my online accounts	3.528	0.964
I have enabled two-factor authentication (2FA) on digital platforms	3.347	1.042
I know how to check if a website is secure before sharing personal data	3.451	0.973
I avoid clicking on suspicious links or attachments	3.618	0.905
I find phishing-detection features in browsers and email platforms easy to use.	3.236	1.061
Composite Mean	**3.440**	**0.989**

The results indicate a moderate to high level of technology adoption, with a composite mean of 3.440, which falls within the "agree" category. This suggests that respondents generally adopt basic cybersecurity practices, although not consistently across all measures. The highest-rated practice was avoiding suspicious links (M = 3.618, SD = 0.905), indicating relatively strong adherence to basic cyber hygiene. The low standard deviation suggests moderate agreement among respondents, implying that this behavior is widely practiced. Similarly, the use of strong passwords (M = 3.528, SD = 0.964) and knowledge of secure websites (M = 3.451, SD = 0.973) also fall within the "agree" range, though with some variability, indicating that while many respondents adopt these practices, consistency is not universal.

However, relatively lower mean scores were observed for the use of two-factor authentication (M = 3.347, SD = 1.042) and the ease of using phishing-detection features

in browsers and email platforms (M = 3.236, SD = 1.061), both of which fall within the moderate category. The comparatively higher standard deviations indicate greater variation in respondents' experiences and adoption levels. These findings suggest that while youth generally recognize the importance of cybersecurity measures, the adoption and effective use of more advanced security features remain inconsistent. This may be attributed to challenges related to usability, technical complexity, or limited awareness, thereby increasing vulnerability to online identity theft and phishing attacks among some respondents.

4.5.2 Correlation Analysis between Technology Adoption and Mitigation

This section examines the relationship between technology adoption and the mitigation of online identity theft and phishing among youth in Westlands Constituency using Pearson's correlation analysis.

Table 4.7

Correlation between Technology Adoption and Mitigation

Variables		**Technology Adoption**	**Mitigation**
Technology Adoption	Pearson Correlation	1.000	
Mitigation of Identity Theft and Phishing	Pearson Correlation	0.587**	1.000
	Sig. (2-tailed)	<.001	
	N	338	338

Note: Correlation is significant at $p < 0.05$ (2-tailed)

The results indicate a moderate to strong positive relationship between technology adoption and mitigation of online identity theft and phishing ($r = 0.587$, $p < 0.001$). This implies that higher levels of adoption of cybersecurity tools and practices are associated with improved ability to prevent or respond to phishing and identity theft. In practical terms, respondents who consistently use antivirus software, strong passwords, secure browsing techniques, and phishing detection features are more likely to exhibit behaviors that reduce exposure to cyber threats. The statistical significance of the relationship further confirms that technology adoption is a key factor in strengthening cybersecurity outcomes among youth.

4.5.3 Predictive Relationship between Technology Adoption and Mitigation

This section presents the results of regression analysis conducted to determine the extent to which technology adoption predicts the mitigation of online identity theft and phishing among youth in Westlands Constituency.

Table 4.8

Regression Results on Technology Adoption and Mitigation of Identity Theft & Phishing

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error
1	0.587	0.345	0.343	0.602

ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	63.957	1	63.957	176.64	<0.001
Residual	121.657	336	0.362		
Total	185.614	337			

Regression Coefficients

Variable	B	Std. Error	Beta	t	Sig.	95% CI for B

(Constant)	1.284	0.176		7.295	<0.001	
Technology Adoption	0.603	0.045	0.587	13.291	<0.001	[0.514, 0.692]

The regression results indicate that technology adoption is a positive and statistically significant predictor of Mitigation of Identity Theft & Phishing ($\beta = 0.587$, $p < .001$). The model explains approximately 34.5% ($R^2 = 0.345$) of the variation in Mitigation of Identity Theft & Phishing, suggesting that technology adoption is a substantial predictor of mitigation outcomes among respondents. The model was statistically significant, $F(1, 336) = 176.640$, $p < .001$. The unstandardized coefficient was also statistically significant ($B = 0.603$, $SE = 0.045$, 95% CI [0.514, 0.692]).

The regression equation derived from the model is:

$$\text{Mitigation} = 1.284 + 0.603(\text{Technology Adoption})$$

The equation indicates that a one-unit increase in technology adoption is associated with a predicted 0.603-unit increase in Mitigation of Identity Theft & Phishing. However, the R^2 value also suggests that other factors contribute to mitigation, supporting the inclusion of additional variables such as cybersecurity education and policy awareness in subsequent analysis.

4.5.4 Qualitative Insights on Technology Adoption

his section presents qualitative insights on technology adoption derived from open-ended responses and supported by document review findings, focusing on user experiences, barriers to adoption, and behavioral patterns influencing the use of cybersecurity practices. Open-ended responses relating to technology adoption were reviewed and coded

according to recurring ideas. Similar codes were grouped into themes reflecting commonly reported cybersecurity practices and barriers to technology adoption. Representative responses were selected to illustrate the themes.

Respondents reported using a range of basic cybersecurity measures, including antivirus software, strong passwords, and cautious handling of suspicious links. Many indicated that their adoption of these practices was influenced by prior exposure to cyber risks or general awareness of online threats. For example, one respondent noted, *"I always avoid clicking unknown links because I have seen people lose money through scams,"* while another stated, *"I use strong passwords especially for my bank apps because I know hackers target those accounts."* These responses suggest that respondents possess basic cybersecurity awareness and tend to adopt reactive protective behaviors. However, the use of advanced tools such as two-factor authentication and phishing detection features was less common. One participant remarked, *"I have heard about 2FA but I don't really know how to activate it."* This observation is consistent with findings from Communications Authority of Kenya (CAK, 2023) and National Crime Research Centre (NCRC, 2023), which indicate that although cyber threat incidents are increasing, the adoption of advanced cybersecurity measures among youth remains limited due to low awareness and inadequate digital skills.

Several barriers to technology adoption also emerged from the qualitative data. Respondents cited lack of awareness, perceived complexity of cybersecurity tools, and reliance on service providers as key challenges. For instance, one respondent stated, *"Some of these security settings are complicated, so I just leave them as default,"* while

another indicated, *"I think companies should handle security, not users."* Additionally, convenience-driven behaviors were evident, as illustrated by the response, *"I use the same password for many accounts because it is easier to remember."* Document review of national frameworks such as the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019) further revealed that while comprehensive policies exist, there is limited translation of these frameworks into practical user-level adoption and awareness. Overall, the qualitative and document-based findings reinforce the quantitative results by demonstrating that while basic cybersecurity practices are present, gaps in knowledge, accessibility, and behavioral consistency limit the effectiveness of technology adoption in mitigating online identity theft and phishing.

4.6 Cybersecurity Education and Mitigation of Online Identity Theft and Phishing

This section examines the relationship between cybersecurity education and the mitigation of online identity theft and phishing among youth in Westlands Constituency. Cybersecurity education in this study refers to the level of awareness, training, knowledge, and confidence that individuals possess in identifying, preventing, and responding to cyber threats.

This analysis is guided by the research objective: to examine the relationship between cybersecurity education and mitigation of online identity theft and phishing among youth in Westlands Constituency, and the corresponding research question: what relationship exists between cybersecurity education and mitigation of online identity theft and phishing among youth in Westlands Constituency?

The section is structured to provide a comprehensive evaluation of this relationship. It begins with descriptive statistics to assess the level of cybersecurity education among respondents, followed by correlation analysis to examine the relationship between cybersecurity education and mitigation. Regression analysis is then conducted to determine the predictive contribution of cybersecurity education to mitigation outcomes. In addition, qualitative insights are integrated to provide deeper understanding of training exposure, awareness gaps, and behavioral responses to cybersecurity risks.

4.6.1 Descriptive Analysis of Cybersecurity Education

A five-point Likert scale was used to measure responses on statements regarding cybersecurity education, where 1.000–1.800 = Strongly Disagree, 1.801–2.600 = Disagree, 2.601–3.400 = Neutral/Moderate, 3.401–4.200 = Agree, and 4.201–5.000 = Strongly Agree.

Table 4.9

Descriptive Statistics for Cybersecurity Education (n = 338)

Statement	Mean	Std. Dev
I have received training (formal/informal) on cybersecurity	3.148	1.084
I can identify phishing emails or fake digital messages	3.236	1.062
I know where to report cybercrime or phishing attempts	2.984	1.117
I follow cybersecurity tips or updates from trusted sources	3.312	1.028
I feel confident in my ability to avoid identity theft online	3.278	1.041
Composite Mean	**3.192**	**1.066**

The findings indicate a moderate level of cybersecurity education, with a composite mean of 3.192, falling within the “neutral/moderate” category. The relatively high standard

deviation (SD = 1.066) suggests variability in responses, indicating unequal levels of exposure to cybersecurity knowledge among respondents. Specifically, the statement on receiving cybersecurity training (M = 3.148, SD = 1.084) indicates that respondents are moderately exposed to formal or informal training, though the relatively high dispersion suggests that such training is not uniformly accessible. The ability to identify phishing emails (M = 3.236, SD = 1.062) also falls within the moderate range, implying that while some respondents possess detection skills, others remain uncertain, increasing vulnerability to cyber threats.

Similarly, knowledge of where to report cybercrime (M = 2.984, SD = 1.117) records the lowest mean and a high standard deviation, indicating both limited awareness and significant inconsistency among respondents. This suggests that many youth are not adequately informed about formal reporting mechanisms, which may hinder effective response to cyber incidents. The statement on following cybersecurity tips (M = 3.312, SD = 1.028) reflects moderate engagement with awareness content, although the variability indicates inconsistent behavioral adoption. Confidence in avoiding identity theft (M = 3.278, SD = 1.041) also falls within the moderate range, suggesting that respondents possess some level of self-efficacy, though not strong enough to ensure consistent protective behavior.

4.6.2 Correlation Analysis between Cybersecurity Education and Mitigation

This section examines the relationship between cybersecurity education and the mitigation of online identity theft and phishing among youth in Westlands Constituency using Pearson's correlation analysis.

Table 4.10

Correlation between Cybersecurity Education and Mitigation

Variables		**Cybersecurity Education**	**Mitigation**
Cybersecurity Education	Pearson Correlation	1.000	
Mitigation of Identity Theft and Phishing	Pearson Correlation	0.641**	1.000
	Sig. (2-tailed)	<.001	
	N	338	338

Note: Correlation is significant at $p < 0.05$ (2-tailed)

The results indicate a strong positive relationship between cybersecurity education and mitigation of online identity theft and phishing ($r = 0.641$, $p < 0.001$). This suggests that increased levels of cybersecurity knowledge, training, and awareness are associated with improved ability to prevent and respond to cyber threats among respondents. In practical terms, individuals who are more informed about identifying phishing attempts, understanding safe online practices, and knowing appropriate response mechanisms are more likely to adopt behaviors that reduce their exposure to identity theft and related cyber risks.

4.6.3 Predictive Relationship between Cybersecurity Education and Mitigation

This section presents the regression analysis results examining the extent to which cybersecurity education predicts the mitigation of online identity theft and phishing among youth in Westlands Constituency.

Table 4. 3:

Regression Results on Cybersecurity Education on Mitigation

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error
1	0.641	0.411	0.409	0.574

ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	76.271	1	76.271	234.364	<.001
Residual	109.343	336	0.325		
Total	185.614	337			

Regression Coefficients

Variable	B	Std. Error	Beta	t	Sig.	95% CI for B
(Constant)	1.102	0.158		6.975	<.001	
Cybersecurity Education	0.672	0.044	0.641	15.309	<.001	[0.586, 0.758]

The regression results indicate that cybersecurity education is a positive and statistically significant predictor of Mitigation of Identity Theft & Phishing ($\beta = 0.641$, $p < .001$). The model explains approximately 41.1% ($R^2 = 0.411$) of the variation in mitigation, indicating that cybersecurity education is a strong predictor of cybersecurity outcomes among respondents. The model was statistically significant, $F(1, 336) = 234.364$, $p < .001$. The unstandardized coefficient was also statistically significant ($B = 0.672$, $SE = 0.044$, 95% CI [0.586, 0.758]).

The regression equation derived from the model is:

$$\text{Mitigation} = 1.102 + 0.672(\text{Cybersecurity Education})$$

This implies that a unit increase in cybersecurity education is associated with a predicted 0.672-unit increase in Mitigation of Identity Theft & Phishing. The positive coefficient indicates that respondents with higher levels of cybersecurity knowledge, awareness, and training tend to report higher perceived effectiveness of mitigation strategies. The relatively higher R^2 value compared to technology adoption suggests that cybersecurity education has a stronger predictive contribution to mitigation outcomes.

4.6.4 Qualitative Insights on Cybersecurity Education

This section presents qualitative insights on cybersecurity education derived from open-ended responses and supported by document review findings, focusing on training exposure, awareness levels, and behavioral responses to cyber threats. Open-ended responses relating to cybersecurity education were reviewed and coded according to recurring ideas. Similar codes were grouped into themes reflecting training exposure, awareness gaps, and response knowledge. Representative responses were selected to illustrate the themes.

Respondents reported varying levels of exposure to cybersecurity education, with most indicating that their knowledge was acquired informally through personal experience, social media, or peer interactions rather than structured training. For instance, one respondent noted, *"I have never had formal training, I just learn from what I see online or when something happens,"* while another stated, *"Most of what I know about cyber threats is from news and social media."* Although some respondents demonstrated the ability to recognize phishing attempts, others expressed uncertainty, with one participant

stating, *"Sometimes it is hard to tell if a message is real or fake."* These responses suggest that while general awareness exists, practical skills in identifying and responding to cyber threats remain inconsistent. Document review of reports from the (CAK, 2023) and the National Crime Research Centre (NCRC, 2023) further indicates that cybersecurity education programs targeting youth remain limited in coverage and practical orientation.

Further insights reveal gaps in knowledge regarding reporting mechanisms and response strategies. Several respondents indicated uncertainty about where to report cyber incidents, with one stating, *"I wouldn't know where to report if I got scammed,"* and another noting, *"I think you just block the person, I don't know if there is anywhere to report."* Document analysis of national frameworks such as the Data Protection Act (2019) and the Computer Misuse and Cybercrimes Act (2018) shows that although legal mechanisms for addressing cybercrime exist, public awareness and accessibility remain limited. Overall, the qualitative and document-based findings reinforce the quantitative results by demonstrating that insufficient training, limited awareness, and low self-efficacy constrain the effectiveness of cybersecurity education in mitigating online identity theft and phishing among youth.

4.7 Policy Awareness and Mitigation of Online Identity Theft and Phishing

This section examines the relationship between policy awareness and the mitigation of online identity theft and phishing among youth in Westlands Constituency. Policy awareness in this study refers to respondents' knowledge of existing cybercrime laws,

understanding of their rights under data protection frameworks, and perceptions of the effectiveness of enforcement mechanisms.

This analysis is guided by the research objective: to examine the relationship between policy awareness and mitigation of online identity theft and phishing among youth in Westlands Constituency, and the corresponding research question: what relationship exists between policy awareness and mitigation of online identity theft and phishing among youth in Westlands Constituency?

The section is structured to provide a comprehensive assessment of this relationship. It begins with descriptive statistics to evaluate the level of awareness and perceptions of cybercrime policies among respondents. This is followed by correlation analysis to determine the relationship between policy awareness and mitigation. Regression analysis is then conducted to assess the predictive contribution of policy awareness to mitigation outcomes. In addition, qualitative insights are integrated to provide deeper understanding of respondents' perceptions of policy effectiveness, trust in enforcement institutions, and challenges related to reporting cybercrime.

This approach enables a holistic evaluation of the relationship between legal and institutional awareness and cybersecurity behavior among youth.

4.7.1 Descriptive Analysis of Policy Awareness

This section presents the descriptive statistics on respondents' level of awareness and perceptions of cybercrime policies and legal frameworks in Kenya. Policy awareness in

this study encompasses knowledge of existing cybercrime laws, understanding of individual rights under data protection regulations, and perceptions of the effectiveness of enforcement mechanisms. Assessing these aspects is critical in determining whether legal and institutional frameworks translate into practical behavioral change among youth in mitigating online identity theft and phishing. A five-point Likert scale was used to measure responses, where 1.000–1.800 = Strongly Disagree, 1.801–2.600 = Disagree, 2.601–3.400 = Neutral/Moderate, 3.401–4.200 = Agree, and 4.201–5.000 = Strongly Agree.

Table 4.12

Descriptive Statistics for Policy Awareness

Statement	Mean	Std. Dev
I am aware of Kenya's cybercrime laws (e.g., CMCA)	2.874	1.112
I understand my rights under the Data Protection Act (2019)	2.931	1.098
I believe government enforcement of cybercrime policies is effective	2.706	1.134
I believe youth-specific cyber policies are needed in Kenya	3.462	1.021
I trust authorities will act on reported cybercrime cases	2.689	1.147
Composite Mean	**2.932**	**1.102**

The findings indicate a low to moderate level of policy awareness, with a composite mean of 2.932, which falls within the "neutral/moderate" category but trends toward disagreement. This suggests that respondents have limited awareness and understanding of cybercrime laws and related legal protections. The relatively high standard deviation (SD = 1.102) indicates substantial variability in responses, implying unequal levels of exposure to policy-related information among respondents. Awareness of cybercrime laws (M = 2.874, SD = 1.112) and understanding of rights under the Data Protection Act (M =

2.931, SD = 1.098) are both moderate, indicating that many respondents are not fully informed about existing legal frameworks. Perceptions of government enforcement (M = 2.706, SD = 1.134) and trust in authorities (M = 2.689, SD = 1.147) are comparatively low, suggesting skepticism regarding institutional effectiveness. Notably, trust in authorities to act on reported cybercrime cases recorded the lowest mean score among all policy awareness indicators. This finding suggests that even where respondents possess some awareness of cybercrime laws and data protection rights, limited confidence in enforcement institutions may discourage reporting of incidents and reduce engagement with formal cybersecurity protection mechanisms. However, the higher mean for the need for youth-specific policies (M = 3.462, SD = 1.021) indicates recognition among respondents that current policy frameworks may not adequately address youth-specific cybersecurity challenges.

4.7.2 Correlation Analysis between Policy Awareness and Mitigation

This section examines the relationship between policy awareness and the mitigation of online identity theft and phishing among youth in Westlands Constituency using Pearson's correlation analysis.

Table 4.13

Correlation between Policy Awareness and Mitigation

Variables		Policy Awareness	Mitigation
Policy Awareness	Pearson Correlation	1.000	
Mitigation of Identity Theft and Phishing	Pearson Correlation	0.463**	1.000
	Sig. (2-tailed)	<.001	
	N	338	338

Correlation is significant at $p < 0.05$ (2-tailed)

The results indicate a moderate positive relationship between policy awareness and mitigation of online identity theft and phishing ($r = 0.463$, $p < 0.001$). This suggests that higher levels of awareness of cybercrime laws, data protection rights, and institutional frameworks are associated with improved ability to prevent and respond to cyber threats. However, the strength of the relationship is lower compared to technology adoption and cybersecurity education, indicating that policy awareness, while important, has a comparatively weaker relationship with mitigation.

4.7.3 Predictive Relationship between Policy Awareness and Mitigation

This section presents the regression analysis results examining the extent to which policy awareness predicts the mitigation of online identity theft and phishing among youth in Westlands Constituency.

Table 4.14

Regression Results on the Predictive Relationship between Policy Awareness and Mitigation

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error
1	0.463	0.214	0.212	0.659

ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	39.79	1	39.79	91.682	<.001
Residual	145.824	336	0.434		
Total	185.614	337			

Regression Coefficients

Variable	B	Std. Error	Beta	t	Sig.	95% CI for B
(Constant)	1.563	0.192		8.141	<.001	
Policy Awareness	0.482	0.050	0.463	9.575	<.001	[0.383, 0.581]

The regression results indicate that policy awareness is a positive and statistically significant predictor of Mitigation of Identity Theft & Phishing ($\beta = 0.463$, $p < .001$). The model explains approximately 21.4% ($R^2 = 0.214$) of the variation in mitigation, suggesting that policy awareness makes a statistically significant predictive contribution, although its explanatory power is relatively lower compared to technology adoption and cybersecurity education. The model was statistically significant, $F(1, 336) = 91.682$, $p < .001$. The unstandardized coefficient was also statistically significant ($B = 0.482$, $SE = 0.050$, 95% CI [0.383, 0.581]).

The regression equation derived from the model is:

$$\text{Mitigation} = 1.563 + 0.482(\text{Policy Awareness})$$

This implies that a unit increase in policy awareness is associated with a predicted 0.482-unit increase in Mitigation of Identity Theft & Phishing. The positive coefficient indicates that respondents who are more aware of cybercrime laws, understand their data protection rights, and are knowledgeable about institutional mechanisms tend to report higher perceived effectiveness of mitigation strategies. However, the relatively lower R^2 value suggests that policy awareness has a weaker predictive contribution to mitigation compared with cybersecurity education and technology adoption.

4.7.4 Qualitative Insights on Policy Awareness

This section presents qualitative insights on policy awareness derived from open-ended responses and supported by document review findings, focusing on respondents' knowledge of cybercrime laws, perceptions of institutional effectiveness, and experiences with reporting mechanisms. Open-ended responses relating to policy awareness were reviewed and coded according to recurring ideas. Similar codes were grouped into themes reflecting awareness of cybercrime laws, trust in enforcement institutions, reporting challenges, and perceptions of youth-specific policy needs. Representative responses were selected to illustrate the themes.

The findings indicate that most respondents have limited awareness of existing cybercrime policies and legal frameworks. While a few participants demonstrated basic familiarity with cyber laws, the majority were either unaware or uncertain about their rights and available protections. For instance, one respondent stated, *"I have heard about cybercrime laws but I don't know what they actually say,"* while another noted, *"I don't really know*

anything about data protection laws." These responses suggest that although legal frameworks exist, their visibility and accessibility among youth remain low.

Further insights reveal low trust in enforcement institutions and reporting mechanisms. Several respondents expressed skepticism regarding the effectiveness of authorities in addressing cybercrime, with one stating, *"Even if you report, nothing will happen,"* and another indicating, *"I don't think reporting helps because these cases are not followed up."* Others were uncertain about where to report incidents, with responses such as, *"I wouldn't know where to report if I got scammed."*

Additionally, respondents expressed a strong perception that current policies do not adequately address youth-specific cybersecurity challenges. One participant remarked, *"There should be more policies focused on young people because we are the most affected,"* while another noted, *"Most of these laws are not explained to us in a way we can understand."* Document review of frameworks such as the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019) indicates that while comprehensive legal provisions exist, there is limited emphasis on youth-centered awareness and implementation strategies. Overall, the qualitative findings indicate limited policy awareness, low confidence in enforcement institutions, uncertainty regarding reporting mechanisms, and perceived need for more accessible youth-focused cybersecurity policy information.

4.8 Joint Predictive Contribution of Technology Adoption, Cybersecurity Education, and Policy Awareness to Mitigation

This section presents the joint predictive contribution of technology adoption, cybersecurity education, and policy awareness to the mitigation of online identity theft and phishing among youth in Westlands Constituency. The analysis provides a comprehensive evaluation of how these variables jointly predict mitigation outcomes.

Table 4.15

Regression Results on the Integrated Predictive Contribution of Technology Adoption, Cybersecurity Education, and Policy Awareness to Mitigation

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error
1	0.721	0.520	0.516	0.517

ANOVA Results

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	96.520	3	32.173	120.611	<.001
Residual	89.094	334	0.267		
Total	185.614	337			

Regression Coefficients

Variable	B	Std. Error	Beta	t	Sig.	95% CI for B
(Constant)	0.842	0.143		5.889	<.001	[0.561, 1.123]
Technology Adoption	0.291	0.041	0.283	7.098	<.001	[0.210, 0.372]
Cybersecurity Education	0.408	0.039	0.396	10.462	<.001	[0.331, 0.485]
Policy Awareness	0.173	0.036	0.169	4.806	<.001	[0.102, 0.244]

The results indicate that the combined model is statistically significant, $F(3, 334) = 120.611$, $p < .001$, and explains approximately 52.0% ($R^2 = 0.520$) of the variation in Mitigation of Identity Theft & Phishing. The adjusted R^2 of 0.516 indicates that the three predictors jointly account for approximately 51.6% of the variation in mitigation after

adjustment for the number of predictors in the model. The remaining 48.0% is associated with factors not included in the model.

The regression equation for the model is:

$$\text{Mitigation} = 0.842 + 0.291(\text{Technology Adoption}) + 0.408(\text{Cybersecurity Education}) + 0.173(\text{Policy Awareness})$$

The findings show that all three variables make positive and statistically significant predictive contributions to Mitigation of Identity Theft & Phishing. Cybersecurity education has the strongest standardized predictive contribution ($\beta = 0.396$, $B = 0.408$, $p < .001$, 95% CI [0.331, 0.485]), followed by technology adoption ($\beta = 0.283$, $B = 0.291$, $p < .001$, 95% CI [0.210, 0.372]). Policy awareness has the smallest, but still statistically significant, predictive contribution ($\beta = 0.169$, $B = 0.173$, $p < .001$, 95% CI [0.102, 0.244]). Thus, when the three predictors are considered simultaneously, cybersecurity education emerges as the strongest predictor of mitigation, followed by technology adoption and policy awareness.

Overall, the results demonstrate that technology adoption, cybersecurity education, and policy awareness jointly predict Mitigation of Identity Theft & Phishing, with the model accounting for a substantial proportion of the variation in mitigation outcomes among the respondents.

4.9 Development of a Cybersecurity Framework for Mitigating Identity Theft and Phishing

This section presents the development of a proposed empirically informed cybersecurity framework based on the findings of the study. The framework integrates technology adoption, cybersecurity education, and policy awareness to provide a structured approach for mitigating online identity theft and phishing among youth in Westlands Constituency.

The development of the framework is grounded in both quantitative and qualitative findings of the study. The regression analysis established that technology adoption, cybersecurity education, and policy awareness jointly and significantly predict Mitigation of Identity Theft & Phishing, with the combined model explaining 52.0% of the variation in mitigation outcomes ($R^2 = 0.520$). Cybersecurity education had the strongest predictive contribution ($\beta = 0.396$), followed by technology adoption ($\beta = 0.283$), while policy awareness had the smallest but statistically significant predictive contribution ($\beta = 0.169$). These findings provide the empirical basis for incorporating the three components into the proposed framework.

Qualitative findings further revealed that respondents rely heavily on basic cybersecurity practices but demonstrate limited adoption of advanced tools due to lack of awareness and perceived complexity. In addition, most respondents acquire cybersecurity knowledge informally, with minimal exposure to structured training programs. Document review of reports from the Communications Authority of Kenya and the National Crime Research Centre also indicated that cybersecurity awareness initiatives targeting youth are limited

in scope, while policy frameworks, though well established, are not effectively translated into user-level awareness and action.

The findings also showed that policy awareness had the smallest predictive contribution to mitigation among the three variables. Respondents demonstrated relatively low levels of awareness of existing cybercrime laws and expressed uncertainty about reporting mechanisms and limited trust in enforcement institutions. These findings indicate a gap between the existence of cybersecurity policies and respondents' awareness and engagement with the available institutional mechanisms.

4.9.1 Proposed Cybersecurity Framework

Based on the empirical findings of the study, a multidimensional cybersecurity framework is proposed to enhance the mitigation of online identity theft and phishing among youth. The framework integrates three interrelated components: cybersecurity education, technology adoption, and policy awareness.

1. Cybersecurity Education (Core Driver)

- Continuous awareness and training programs
- Integration of cybersecurity education in schools and youth programs
- Practical training on phishing detection and response

2. Technology Adoption (Protective Mechanism)

- Promotion of security tools such as:
    - Two-factor authentication (2FA)
    - Antivirus software and firewalls

    - Secure browsing practices
- Simplification and user-friendly implementation of cybersecurity tools

3. Policy Awareness (Institutional Support)

- Increased awareness of key legal frameworks such as:
    - Computer Misuse and Cybercrimes Act (2018)
    - Data Protection Act (2019)
- Improved accessibility of cybercrime reporting mechanisms
- Strengthening trust in enforcement and regulatory institutions

Framework Logic

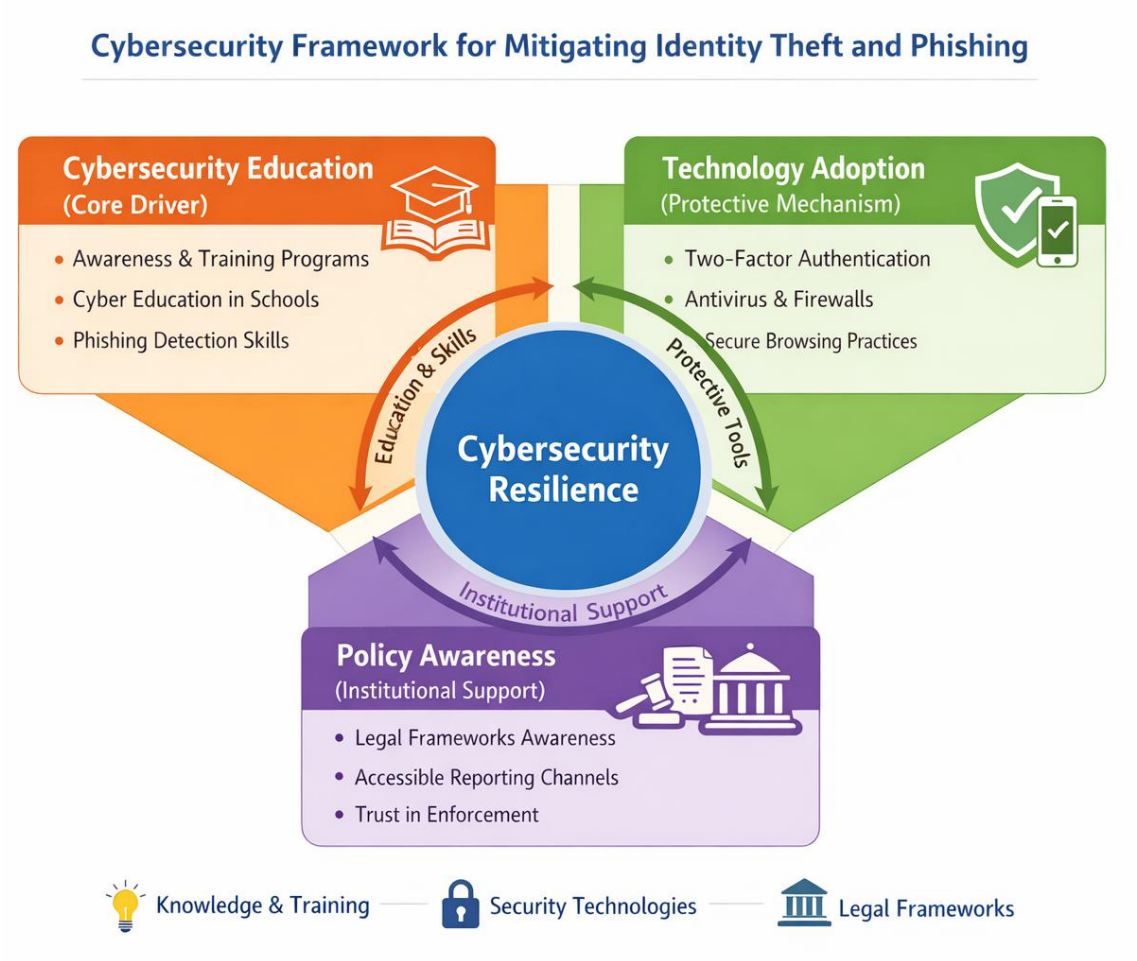
The proposed framework integrates behavioral, technological, and institutional dimensions identified in the study. Cybersecurity education represents the strongest predictor in the integrated regression model and focuses on strengthening users' knowledge, awareness, and skills in identifying and responding to cyber threats. Technology adoption provides the technological dimension through the use of protective tools and safe online practices. Policy awareness provides the institutional dimension by enhancing users' understanding of relevant legal frameworks, reporting mechanisms, rights, and available institutional support.

The three components are presented as complementary elements of the proposed framework. The study findings showed that each component made a positive and statistically significant predictive contribution to Mitigation of Identity Theft & Phishing

when considered jointly. Their integration therefore reflects the empirical pattern identified in the study rather than treating any single component as sufficient on its own.

Figure 4. 1

Proposed Empirically Informed Cybersecurity Framework for Mitigating Identity Theft and Phishing



The proposed framework provides a structured and integrated approach for policymakers, educators, and technology providers to design targeted interventions aimed at reducing cybercrime among youth. It emphasizes that effective mitigation of identity theft and phishing requires not only access to technological tools but also adequate user knowledge and strong institutional support systems.

Overall, the framework represents a proposed empirically informed model derived from the study findings. It should therefore be interpreted as a conceptual integration of the factors supported by the study rather than as a separately validated intervention model.

4.10 Discussion of Findings

This section discusses the study findings in relation to the research objectives, existing literature, and relevant theoretical perspectives.

4.10.1 Technology Adoption and Mitigation of Online Identity Theft and Phishing

The first objective of the study sought to examine the relationship between technology adoption and mitigation of online identity theft and phishing among youth in Westlands Constituency. The findings revealed a positive and statistically significant relationship between technology adoption and Mitigation of Identity Theft & Phishing. However, the level of technology adoption was found to be moderate, with respondents primarily relying on basic practices such as strong passwords, antivirus software, and avoidance of suspicious links, while the use of advanced tools such as two-factor authentication and phishing detection features remained inconsistent.

These findings align with existing literature, which indicates that although users are generally aware of cybersecurity tools, their adoption tends to be selective and skewed toward less complex practices. Mbaya and Muriuki (2023) found that Kenyan youth commonly adopt basic security behaviors but exhibit low uptake of advanced tools due to limited technical knowledge and perceived complexity. Similarly, Sitienei (2025) reported that the adoption of cybersecurity technologies is often inconsistent, with users failing to

implement comprehensive protection strategies despite being aware of potential risks. This suggests that awareness alone may be insufficient to explain full adoption, as behavioral and usability factors are also associated with technology use.

The moderate adoption of advanced tools observed in this study is further supported by Alkaabi et al. (2023), who established that users are more likely to adopt cybersecurity measures that are simple and easy to implement, while avoiding those perceived as complex or time-consuming. In addition, Afzal et al. (2024) found that perceived ease of use and user competence are significantly associated with technology adoption, with low self-efficacy acting as a barrier to the use of more advanced protective tools. This reinforces the importance of considering not only the availability of cybersecurity technologies but also users' ability and willingness to utilize them consistently.

The findings also show that basic cybersecurity practices, such as avoiding suspicious links and using strong passwords, are more widely adopted because they are easier to understand and apply. This is consistent with Desolda et al. (2021), who found that users respond more effectively to visible and immediate threats compared to less tangible risks. However, reliance on basic practices alone may not provide sufficient protection against increasingly sophisticated cyber threats. Jibril et al. (2020) emphasized that effective mitigation requires a layered approach that integrates both basic and advanced security mechanisms.

From a theoretical perspective, these findings are consistent with the assumptions of the Routine Activity Theory (Cohen & Felson, 1979), which posits that the presence of

capable guardianship reduces the likelihood of victimization. In this context, cybersecurity technologies such as antivirus software, secure browsing tools, and authentication mechanisms represent protective measures. However, the moderate and inconsistent adoption observed suggests that such technological guardianship is not uniformly applied among respondents. This is consistent with Mbaya and Muriuki (2023), who noted that partial adoption of cybersecurity measures leaves users exposed despite having access to protective tools.

Overall, the findings indicate that technology adoption is positively associated with Mitigation of Identity Theft & Phishing. However, the moderate and inconsistent adoption of advanced tools suggests the importance of interventions that promote access to cybersecurity technologies, enhance user capacity, simplify implementation, and encourage consistent adoption.

4.10.2 Cybersecurity Education and Mitigation of Online Identity Theft and Phishing

The second objective of the study sought to examine the relationship between cybersecurity education and mitigation of online identity theft and phishing among youth in Westlands Constituency. The findings revealed a positive and statistically significant relationship between cybersecurity education and mitigation. In the integrated regression model, cybersecurity education also emerged as the **strongest predictor** among the three study variables ($\beta = 0.396$, $p < .001$).

The results further showed that respondents exhibited moderate levels of cybersecurity education, with most relying on informal sources such as social media, personal experiences, and peer learning rather than structured training programs. This suggests that while general awareness of cyber threats exists, it lacks depth and practical orientation. These findings are consistent with Ngunjiri (2024), who found that many youth acquire cybersecurity knowledge informally, resulting in limited practical skills in detecting and responding to sophisticated threats. Similarly, Gan and Liew (2022) established that informal awareness does not adequately equip users with the competencies required to effectively mitigate cyber risks.

The study also found gaps in critical areas such as phishing detection and knowledge of reporting mechanisms, indicating that respondents have limitations in some of the practical skills relevant to mitigation. This aligns with Baraković and Baraković Husić (2023), who reported that although individuals may recognize common cyber threats, their ability to accurately identify and respond to phishing attacks remains limited due to insufficient training. In addition, Parsons et al. (2022) observed that cybersecurity education is significantly associated with improved threat recognition and response behavior, emphasizing the importance of structured and skills-based training programs in enhancing user resilience.

The relatively strong association between cybersecurity education and mitigation observed in this study is consistent with findings by Zulkiplee et al. (2025), who established that cybersecurity awareness and training are important predictors of protective behavior in digital environments. Similarly, Bada et al. (2019) emphasized the

importance of structured awareness programs in strengthening cybersecurity practices and reducing susceptibility to phishing attacks. These findings indicate the relevance of cybersecurity knowledge, attitudes, perceptions, and behavioral skills to mitigation outcomes.

From a theoretical perspective, these findings are consistent with the Health Belief Model (Rosenstock, 1974) and the Protection Motivation Theory (Rogers, 1975), which emphasize that protective behavior is associated with individuals' knowledge, perceptions of risk, and confidence in their ability to respond effectively. The moderate levels of cybersecurity education observed suggest that although respondents have some awareness, gaps in knowledge and self-efficacy may limit their adoption of protective measures.

Overall, the findings indicate that cybersecurity education is positively associated with Mitigation of Identity Theft & Phishing and had the strongest predictive contribution in the integrated model. The reliance on informal knowledge sources and limited exposure to structured training highlight the importance of comprehensive education programs focusing on practical skills, threat detection, and appropriate response mechanisms.

4.10.3 Policy Awareness and Mitigation of Online Identity Theft and Phishing

The third objective of the study sought to examine the relationship between policy awareness and mitigation of online identity theft and phishing among youth in Westlands Constituency. The findings revealed a positive and statistically significant relationship between policy awareness and mitigation. In the integrated regression model, policy

awareness made the smallest but statistically significant predictive contribution ($\beta = 0.169$, $p < .001$) compared with technology adoption and cybersecurity education.

The results further showed that respondents exhibited low to moderate levels of policy awareness, particularly in relation to knowledge of cybercrime laws, understanding of data protection rights, and awareness of reporting mechanisms. In addition, respondents expressed low levels of trust in enforcement institutions, which may hinder the effectiveness of policy frameworks in influencing behavior. These findings are consistent with Agina (2022), who reported that limited awareness of cybercrime laws among Kenyan youth reduces their ability to utilize legal protections and reporting systems. Similarly, Chizanga et al. (2022) found that low trust in enforcement institutions discourages individuals from reporting cyber incidents, thereby weakening the effectiveness of policy interventions.

The relatively weaker predictive relationship between policy awareness and mitigation observed in this study is further supported by findings from the National Crime Research Centre (2022), which indicate that despite the existence of comprehensive legal frameworks, public awareness and utilization of these mechanisms remain low. In addition, reports from the CAK, (2023) highlight that cybercrime policies are often underutilized due to limited public understanding and lack of confidence in enforcement processes. This suggests that the presence of legal frameworks alone is insufficient to influence behavior unless accompanied by effective awareness and trust-building measures.

The findings also revealed that respondents perceive existing policies as inadequate in addressing youth-specific cybersecurity challenges, indicating a gap between policy design and user needs. This aligns with recent studies which emphasize that policy frameworks need to be context-specific and user-centered to achieve meaningful behavioral outcomes. Without targeted communication and engagement strategies, policy awareness may not readily translate into practical mitigation behavior.

From a theoretical perspective, these findings are consistent with Institutional Theory (DiMaggio & Powell, 1983), which emphasizes the role of institutional structures, rules, and norms in shaping behavior. The low levels of awareness and trust observed in this study suggest that respondents have limited engagement with existing cybersecurity policies and institutional mechanisms.

Overall, the findings indicate that policy awareness is positively associated with Mitigation of Identity Theft and Phishing, although it made the smallest predictive contribution among the three variables in the integrated model. The relatively low levels of awareness, limited trust in enforcement institutions, and challenges associated with policy communication highlight the importance of enhanced awareness, accessible reporting mechanisms, and greater public engagement with cybersecurity institutions.

4.10.4 Integrated Discussion of Technology Adoption, Cybersecurity Education, and Policy Awareness

The final objective of the study sought to examine the combined predictive contribution of technology adoption, cybersecurity education, and policy awareness to Mitigation of

Identity Theft & Phishing among youth. The integrated regression model was statistically significant, $F(3, 334) = 120.611$, $p < .001$, and explained 52.0% of the variation in mitigation outcomes ($R^2 = 0.520$; adjusted $R^2 = 0.516$). The findings therefore indicate that the three variables jointly provide substantial predictive information regarding mitigation outcomes.

Among the three variables, cybersecurity education made the strongest standardized predictive contribution ($\beta = 0.396$, $p < .001$), followed by technology adoption ($\beta = 0.283$, $p < .001$), while policy awareness made the smallest but statistically significant contribution ($\beta = 0.169$, $p < .001$). These results suggest that cybersecurity education is particularly relevant to mitigation when the three variables are considered simultaneously.

The relatively stronger predictive contribution of cybersecurity education is consistent with Ngunjiri (2024), who established that digital literacy and cybersecurity awareness are important in users' adoption of protective behaviors. Similarly, Gan and Liew (2022) found that users with higher levels of cybersecurity knowledge are more likely to effectively utilize technological tools and respond appropriately to cyber threats. The present study, however, did not test whether cybersecurity education mediates or moderates the relationships involving technology adoption or policy awareness. The findings are therefore interpreted in terms of their respective predictive contributions rather than indirect effects.

The statistically significant contribution of technology adoption in the combined model reinforces the relevance of cybersecurity tools to mitigation practices. However, its

comparatively smaller standardized coefficient than cybersecurity education indicates that cybersecurity education had the stronger predictive contribution when the other variables were controlled. This finding is consistent with Parsons et al. (2022), who observed that users' ability to understand and correctly apply cybersecurity technologies is relevant to protective behavior. Similarly, Afzal et al. (2024) emphasized user competence and perceived ease of use in explaining technology adoption.

The comparatively smaller predictive contribution of policy awareness indicates that legal and institutional awareness remains relevant, although its contribution was lower than those of cybersecurity education and technology adoption. This aligns with findings by Agina (2022), who noted that policy frameworks have limited practical relevance when users lack awareness or trust in enforcement institutions. In addition, evidence from the CAK, (2023) suggests that engagement with cybercrime policies is constrained by low public awareness and limited understanding of legal provisions. This highlights the gap between policy existence and practical engagement at the user level.

Taken together, the integrated findings show that cybersecurity education, technology adoption, and policy awareness make complementary and statistically significant predictive contributions to Mitigation of Identity Theft & Phishing. Cybersecurity education addresses knowledge and skills, technology adoption represents the use of protective technological measures, while policy awareness captures respondents' knowledge and perceptions of relevant legal and institutional mechanisms. The findings therefore provide empirical support for incorporating all three dimensions into the

proposed cybersecurity framework, without implying causal or interdependent relationships that were not directly tested.

From a theoretical perspective, the findings illustrate the relevance of the theoretical perspectives underpinning the study. The relationship involving cybersecurity education is consistent with the Health Belief Model (Rosenstock, 1974) and Protection Motivation Theory (Rogers, 1975), which emphasize knowledge, perceived risk, and self-efficacy in protective behavior. Technology adoption is consistent with the principles of Routine Activity Theory (Cohen & Felson, 1979), where protective tools may function as capable guardianship. The relationship involving policy awareness can be interpreted through Institutional Theory (DiMaggio & Powell, 1983), which emphasizes the role of institutional structures, rules, and norms in shaping behavior.

Overall, the findings indicate that an integrated consideration of cybersecurity education, technology adoption, and policy awareness provides a more comprehensive understanding of Mitigation of Identity Theft & Phishing among youth. The statistically significant contributions of all three variables provide the empirical basis for their inclusion in the proposed empirically informed cybersecurity framework developed in this study.

4.11 Summary of the Chapter

This chapter presented the analysis and discussion of findings on the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency. The findings showed that technology adoption had a positive and statistically significant relationship

with mitigation, although adoption levels were moderate. Cybersecurity education emerged as the strongest predictor, highlighting the relevance of knowledge and training to mitigation. Policy awareness had a positive but comparatively weaker predictive contribution, mainly in the context of low awareness and limited trust in institutions. The integrated analysis showed that cybersecurity education, technology adoption, and policy awareness jointly predicted mitigation. The findings also informed the development of the proposed empirically informed cybersecurity framework.

CHAPTER FIVE: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary, conclusions, and recommendations of the study on the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency. It synthesizes the key findings in relation to the study objectives, draws conclusions based on the empirical results, and provides recommendations for policy, practice, and future research.

5.2 Summary of the Study

The purpose of this study was to examine the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County. The study was guided by the specific objectives of assessing the relationship between technology adoption and mitigation of online identity theft and phishing, examining the relationship between cybersecurity education and mitigation, examining the relationship between policy awareness and mitigation, determining the combined predictive contribution of technology adoption, cybersecurity education and policy awareness to mitigation, and developing an empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth. A descriptive correlational research design was adopted, and data were collected from 338 respondents using structured questionnaires,

complemented by qualitative responses and document review. Data analysis involved descriptive statistics, Pearson correlation analysis, and multiple regression analysis.

With regard to technology adoption, the study founda positive and statistically significant relationship with Mitigation of Identity Theft & Phishing. The findings indicated that respondents moderately adopted cybersecurity practices, with higher use of basic measures such as strong passwords, antivirus software, and avoidance of suspicious links. However, the adoption of more advanced tools such as two-factor authentication and phishing detection features was inconsistent. The findings therefore indicate that higher technology adoption was associated with higher levels of Mitigation of Identity Theft & Phishing.

In relation to cybersecurity education, the study showed a positive and statistically significant relationship with Mitigation of Identity Theft & Phishing. Respondents exhibited moderate levels of cybersecurity education, with most knowledge acquired through informal channels rather than structured training programs. Gaps were identified in practical areas such as phishing detection and knowledge of reporting mechanisms. In the integrated regression model, cybersecurity education recorded the strongest standardized predictive contribution among the three study variables.

Regarding policy awareness, the study found a positive and statistically significant relationship with Mitigation of Identity Theft & Phishing. The findings revealed low to moderate levels of awareness of cybercrime laws, data protection rights, and reporting mechanisms. In addition, respondents expressed limited trust in enforcement institutions.

In the integrated regression model, policy awareness recorded the smallest, but statistically significant, predictive contribution among the three study variables.

The integrated analysis showed that technology adoption, cybersecurity education, and policy awareness jointly and significantly predicted Mitigation of Identity Theft & Phishing. The three variables jointly accounted for 52.0% of the variation in mitigation ($R^2 = 0.520$). These findings provided the empirical basis for integrating technology adoption, cybersecurity education, and policy awareness into the proposed empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth.

5.3 Conclusions

This section presents conclusions drawn from the study findings in relation to each objective.

5.3.1 Technology Adoption

The study concludes that technology adoption is positively associated with the mitigation of online identity theft and phishing among youth in Westlands Constituency. However, the moderate and inconsistent adoption of advanced security tools indicates that the availability of cybersecurity technologies does not necessarily correspond with their consistent use. Consequently, strengthening mitigation requires greater and more consistent adoption of appropriate cybersecurity tools and practices among youth.

5.3.2 Cybersecurity Education

The study concludes that cybersecurity education is an important dimension in the mitigation of online identity theft and phishing among youth. The reliance on informal sources of cybersecurity knowledge indicates a need for more structured and practical cybersecurity education that equips youth with relevant knowledge and skills for identifying and responding to online threats. Cybersecurity education is therefore particularly relevant within an integrated approach to mitigating identity theft and phishing.

5.3.3 Policy Awareness

The study concludes that policy awareness is positively associated with the mitigation of online identity theft and phishing, although its predictive contribution is comparatively smaller than those of cybersecurity education and technology adoption. Limited knowledge of cybercrime laws, reporting mechanisms and data protection rights, together with low confidence in enforcement institutions, indicates a gap between the existence of cybersecurity policies and youth engagement with the available institutional mechanisms. Greater accessibility and awareness of these mechanisms are therefore important within the broader mitigation framework.

5.3.4 Integrated Conclusion

The study concludes that technology adoption, cybersecurity education and policy awareness provide complementary dimensions for understanding the mitigation of online identity theft and phishing among youth. None of the three dimensions should be considered independently sufficient based on the findings of this study. Their statistically

significant predictive contributions provide the empirical basis for their integration into the proposed empirically informed cybersecurity framework. The framework therefore represents a structured integration of the technological, educational and policy dimensions identified by the study rather than a separately validated intervention model.

5.4 Recommendations

This section presents recommendations based on the study findings, focusing on practical interventions to enhance the mitigation of online identity theft and phishing among youth.

5.4.1 Recommendations on Policy and Practice

First, policymakers and government agencies should strengthen cybersecurity awareness by developing targeted and youth-friendly communication strategies on cybercrime laws, data protection rights, and reporting mechanisms. There is need to simplify legal information and disseminate it through platforms commonly used by youth, such as social media and mobile applications. In addition, enforcement agencies should improve responsiveness and visibility in handling cybercrime cases in order to build public trust and encourage reporting. Policies should also incorporate youth-specific cybersecurity programs to address the unique risks associated with high digital engagement.

Second, educational institutions should integrate structured cybersecurity education into formal learning systems, particularly at secondary, tertiary, and university levels. This should go beyond theoretical knowledge to include practical training on phishing detection, secure online behavior, and incident response. Continuous awareness programs,

workshops, and collaborations with cybersecurity experts should be implemented to enhance students' competencies and promote responsible digital behavior.

Third, technology providers and digital platforms should enhance the usability and accessibility of cybersecurity tools. This includes simplifying the activation and use of features such as two-factor authentication, providing clear user guidance, and incorporating real-time alerts for suspicious activities. Platforms should also embed cybersecurity awareness prompts and educational content within their systems to encourage users to adopt protective measures consistently. This recommendation is supported by Protection Motivation Theory (PMT), particularly the coping appraisal construct, which suggests that individuals are more likely to adopt protective behaviors when they perceive security measures as effective and believe they can easily implement them. Simplifying cybersecurity features and providing user-friendly guidance can therefore enhance users' self-efficacy and increase the likelihood of adopting protective technologies against online identity theft and phishing.

Finally, youth and individual users should be encouraged to adopt comprehensive cybersecurity practices by combining basic and advanced security measures. This includes consistent use of strong passwords, enabling multi-factor authentication, verifying online sources, and avoiding suspicious links. Users should also actively seek credible cybersecurity information and utilize formal reporting channels when exposed to cyber threats.

5.4.2 Recommendations for Further Research

The study recommends that future research should explore additional factors influencing cybersecurity behavior, such as psychological, cultural, and socio-economic determinants. Further studies can also examine the effectiveness of specific cybersecurity interventions, such as training programs or awareness campaigns, in improving mitigation outcomes.

In addition, future research should consider longitudinal designs to assess changes in cybersecurity behavior over time, as well as comparative studies across different regions or demographic groups to enhance generalizability. Researchers may also explore the role of emerging technologies such as artificial intelligence in strengthening cybersecurity and mitigating identity theft and phishing.

5.5 Limitations of the Study

The study was limited to youth aged 18–35 years in Westlands Constituency, Nairobi County. Consequently, the findings reflect the characteristics and experiences of respondents within this specific geographical and demographic context and may not necessarily be generalized to youth in other constituencies or counties with different socio-economic and digital environments.

The study adopted a descriptive correlational research design and collected data at a single point in time. Although the analysis established statistically significant relationships and predictive contributions among the study variables, the design did not permit conclusions about causal relationships between technology adoption, cybersecurity education, policy awareness, and Mitigation of Identity Theft & Phishing.

The study also relied primarily on self-reported questionnaire responses. The findings therefore reflect respondents' reported technology adoption, cybersecurity education, policy awareness, and perceptions of the effectiveness of mitigation strategies. Although qualitative responses and document review provided supplementary contextual information, they did not eliminate the limitations associated with self-reported data.

5.6 Contribution to Knowledge

The study contributes to knowledge by providing empirical evidence on the relationships between technology adoption, cybersecurity education, policy awareness, and Mitigation of Identity Theft & Phishing among youth in Westlands Constituency. Rather than examining these dimensions independently, the study demonstrates their complementary predictive contributions within a single analytical model.

The study further contributes by integrating technology adoption, cybersecurity education, and policy awareness into a proposed empirically informed cybersecurity framework for mitigating online identity theft and phishing among youth. The framework provides a structured representation of the technological, educational, and policy dimensions identified through the study findings. It therefore extends understanding of youth cybersecurity mitigation by bringing these dimensions together within the specific context of Westlands Constituency, Nairobi County.

REFERENCES

African Union Commission. (2024). *Africa cyber security report 2024*. African Union Commission. https://au.int/

Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., & Shoeb, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: an integrated model approach. *Journal of Financial Services Marketing*, *29*(4), 1503-1523. https://doi.org/10.1057/s41264-024-00279-3

Agina, E. M. (2022). *Efficacy of the cyber security legal framework in addressing cybercrime: A focus on Kenya* [Master's thesis, University of Nairobi]. http://erepository.uonbi.ac.ke/handle/11295/164624

Ahmad, M. A., Wisdom, D. D., & Isaac, S. (2020). An empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. *Advances in Multidisciplinary & Scientific Research Journal Publication, 26*(1), 73–84. https://doi.org/10.22624/iSTEAMS/V26P10-IEEE-NG-TS

Al-Badayneh, D. M., Mehawesh, S. S., Alkhater, J. A., Al Qahtani, H. M., & Al Dosari, H. M. (2024). The Relationship between Knowledge Awareness about Qatari Cybersecurity Law, Victimization, and Perpetration Experience: Some Applications of Routine Activities Theory. *Contemp. Readings L. & Soc. Just.*, *16*, 1115.https://cybersecurityjournal.info/uploads/archivepdf/2890The_Relationship_between_Cyber_Opportunity__Low_Self_Control__Cyber_Resilience_and_Cybercrime%20(4)%20(2).pdf

Alkaabi, A., Mohay, G., McAlaney, J., & Ali, R. (2023). Cybercrime awareness and victimisation: A systematic review. *Computers & Security, 126*, 103057. https://doi.org/10.1016/j.cose.2022.103057

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv. https://doi.org/10.48550/arXiv.1901.02672

Baharuddin, M. F., Jalil, A., Amin, Z. M., Rahmad, F., & Shuhidan, S. M. (2025). Digital literacy and cybersecurity in higher education: The unseen power of academic librarians. *International Journal of Evaluation and Research in Education*, *14*(6), 4404-4417. https://doi.org/10.11591/ijere.v14i6.34916

Baraković, S., & Baraković Husić, J. (2023). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A*

Global Perspective, 32(5), 347–370. https://doi.org/10.1080/19393555.2022.2088428

Baral, G. (2021). *Building confidence not to be phished: Conceptualising user self-efficacy in phishing threat avoidance behaviour* [Doctoral dissertation, UNSW Sydney].https://repository.unsworks.unsw.edu.au/server/api/core/bitstreams/3a054fd2-3518-441e-b561-54eaae92f1f2/content

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588. https://doi.org/10.3390/educsci14060588

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

British Psychological Society. (2014). *Code of human research ethics* (2nd ed.). https://www.bps.org.uk/guideline/code-human-research-ethics

Chan-Tin, E., Stalans, L., Johnston, S., Reyes, D., & Kennison, S. (2022). Predicting phishing victimization: Roles of protective and vulnerable strategies and decision-making styles. In *Proceedings of the Fifth International Workshop on Systems and Network Telemetry and Analytics* (pp. 35–42). Association for Computing Machinery. https://doi.org/10.1145/3526064.3534107

Chizanga, M. K., Agola, J., & Rodrigues, A. (2022). Factors affecting cyber security awareness in combating cyber crime in Kenyan public universities. *International Research Journal of Innovations in Engineering and Technology*, *6*(1), 54. https://doi.org/10.47001/IRJIET/2022.601011

Choi, K.-S. (2021). Applying lifestyle-routine activity theory to cybercrime victimization. *Journal of Crime and Justice, 44*(4), 441–459. https://doi.org/10.1080/0735648X.2020.1869533

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Communications Authority of Kenya. (2023). *National KE-CIRT/CC cybersecurity report: Quarter 1, 2023/2024*. https://www.ca.go.ke

Communications Authority of Kenya. (2024). *Annual report for the financial year 2023–2024*. Communications Authority of Kenya. https://www.ca.go.ke/sites/default/files/2025-11/Annual%20Report%202023-2024%20Final.pdf

Computer Misuse and Cybercrimes Act, No. 5 (2018). https://new.kenyalaw.org/akn/ke/act/2018/5/eng%402022-12-31

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). Sage.

Cybersecurity Ventures. (2023). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. https://cybersecurityventures.com/cybercrime-report/

Data Protection Act, No. 24 (2019). https://new.kenyalaw.org/akn/ke/act/2019/24/eng

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Delso-Vicente, A. T., Díaz-Marcos, L., & Peña-García, N. (2025). Factors influencing employee compliance with information security policies: A systematic literature review. *Future Business Journal, 11*(1), Article 22. https://doi.org/10.1186/s43093-025-00418-5

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & García de Blanes-Sebastián, M. (2025). Factors influencing employee compliance with information security policies: A systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal, 11*, Article 28. https://doi.org/10.1186/s43093-025-00452-7

Desetty, A. G., Jangampet, V. D., & Pulyala, S. R. (2020). Phishing attacks: Evolving techniques, emerging trends, and countermeasure strategies. *International Journal for Innovative Engineering and Management Research*, *9*(12), 985-991. https://www.researchgate.net/publication/376645699_Phishing_Attacks_Evolving_Techniques_Emerging_Trends_and_Countermeasure_Strategies

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), 1-35. https://doi.org/10.1145/3469886

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). (2021). *Digital transformation and cybersecurity in Africa: Opportunities and challenges*. https://www.giz.de

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160. https://doi.org/10.2307/2095101

Du, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: determinants of preventative security behaviors. *Journal of Cybersecurity*, *10*(1), tyae012. https://doi.org/10.1093/cybsec/tyae012

Esteves, N. (2023). *Influence of Phishing Awareness on Remote Employee's Security Protection Behavior* [Doctoral dissertation, Capella University]. https://search.proquest.com/openview/c4869da9680e71441caf8834e748238a/1?pq-origsite=gscholar&cbl=18750&diss=y

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Finkelhor, D., Walsh, K., & Jones, L. (2021). Youth internet safety education: Aligning programs with the evidence base. *Trauma, Violence, & Abuse, 22*(4), 695–705. https://doi.org/10.1177/1524838019882325

Finklea, K. M., & Theohary, C. A. (2020). *Cybercrime: Conceptual issues for Congress and U.S. law enforcement* (CRS Report No. R42547). Congressional Research Service. https://crsreports.congress.gov

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2019). *How to design and evaluate research in education* (10th ed.). McGraw-Hill Education. https://studentebookhub.com/wp-content/uploads/2024/preview/9781259913839.pdf

Gan, C. L., & Liew, T. W. (2022). Phishing victimization among Malaysian young adults: Cyber routine activities theory. *Journal of Adult Protection, 24*(3), 193–210. https://doi.org/10.1108/JAP-07-2021-0032

Gay, L. R., Mills, G. E., & Airasian, P. (2012). *Educational research: Competencies for analysis and applications* (10th ed.). Pearson. https://bgdcollege.in/uploads/431Gay-E%20Book%20Educational%20Research-2012.pdf

Girma, A., Muir, A., & Brown, K. (2024). Reviewing the effectiveness of multi-factor authentication in preventing phishing attacks. In *Lecture Notes in Computer Science* (Vol. 14391, pp. 578–589). Springer. https://doi.org/10.1007/978-3-031-73128-0_40

Glanz, K., Rimer, B. K., & Viswanath, K. (2008). *Health behavior and health education: Theory, research, and practice* (4th ed.). Jossey-Bass. https://transformationalchange.pbworks.com/f/HealtBehavior-Education.pdf

Goncalves, V. (2024). *An assessment of the effects of COVID-19 stay-at-home orders on street and cybercrimes in a Brazilian city* [Doctoral dissertation, Sam Houston State University]. Texas Digital Library. https://tdl-ir.tdl.org/items/e8c34b97-b0d0-4181-923d-f60b84019e44

Government of Kenya. (2022). *National cybersecurity strategy 2022–2027*. National Computer and Cybercrimes Coordination Committee. https://nc4.go.ke/storage/2022/09/KENYA-CYBERSECURITY-STRATEGY-2022-2027.pdf

Greenwood, R., Oliver, C., Lawrence, T. B., & Meyer, R. E. (2017). *The SAGE handbook of organizational institutionalism* (2nd ed.). SAGE Publications. https://doi.org/10.4135/9781526415066

Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal*, *36*(3), 472-497. https://doi.org/10.1057/s41284-022-00350-5

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge. https://doi.org/10.4324/9781315775944

International Telecommunication Union. (2024). *Global cybersecurity index 2024*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Ismaeel, S. (2025). The Impact of Digital Literacy on Cybercrime Awareness, Victimization, and Prevention Measures: A Study of Cyberbullying in Saudi Arabia. *Pakistan Journal of Criminology*, *17*(1), 77. https://doi.org/10.62271/pjc.171.77.96

Jibril, A. B., Kwarteng, M. A., Botchway, R. K., Bode, J., & Chovancova, M. (2020). The impact of online identity theft on customers' willingness to engage in e-banking transaction in Ghana: A technology threat avoidance theory. *Cogent Business & Management*, *7*(1), 1832825. https://doi.org/10.1080/23311975.2020.1832825

Kabaya, M., & Kageni, M. (2024). *Cybersecurity in the wake of the Fourth Industrial Revolution in Kenya* (Discussion Paper No. 326). Kenya Institute for Public Policy Research and Analysis. https://repository.kippra.or.ke/items/88da1ca2-55f1-45a7-aca2-efc4ef01523f

Kenya National Bureau of Statistics. (2024). *Economic survey 2024*. Kenya National Bureau of Statistics. KNBS Economic Survey 2024

Kenya National Bureau of Statistics. (2019). *2019 Kenya population and housing census: Volume I—Population by county and sub-county*. https://www.knbs.or.ke/reports/kenya-census-2019/

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International.

Mbaya, K., & Muriuki, P. (2023). *Assessment of information communication technology crimes and offences in Kenya*. National Crime Research Centre. https://www.crimeresearch.go.ke/wp-content/uploads/2024/07/INFORMATION-COMMUNICATION-TECHNOLOGY-CRIMES-AND-OFFENCES-IN-KENYA.pdf

McMillan, J. H., & Schumacher, S. (2014). *Research in education: Evidence-based inquiry* (7th ed.). Pearson.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. https://doi.org/10.1086/226550

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications. https://eric.ed.gov/?id=ED565763

Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior, 158*, 108274. https://doi.org/10.1016/j.chb.2024.108274

Mugarura, N., & Ssali, E. (2021). Anti-money laundering and cybercrime regulation. *Journal of Money Laundering Control, 24*(4), 791–804. https://doi.org/10.1108/JMLC-11-2020-0133

Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. ACTS Press.

Mwamba, F., & Mjema, E. A. (2024). The Effects of Phishing Attacks on Mobile Phone Users in Tanzania: A Case of Kariakoo Market, Dar es Salaam. *African Journal of Empirical Research*, *5*(4), 665-674. https://doi.org/10.51867/ajernet.5.4.54

National Computer and Cybercrimes Coordination Committee. (2022). *National cybersecurity strategy 2022–2027*. Government of Kenya. https://nc4.go.ke/regulations/national-cybersecurity-strategy-2022-2027/

National Crime Research Centre. (2023). *Information communication technology crimes and offences in Kenya*. https://www.crimeresearch.go.ke/wp-content/uploads/2024/07/INFORMATION-COMMUNICATION-TECHNOLOGY-CRIMES-AND-OFFENCES-IN-KENYA.pdf

Ngunjiri, N. (2024). Technological Developments and Innovations Influence Cybercrime Rise in Juja Sub-County. *National Security*. https://www.researchgate.net/publication/385516980_TECHNOLOGICAL_DEVELOPMENTS_AND_INNOVATIONS_INFLUENCE_CYBERCRIME_RISE_IN_JUJA_SUB-COUNTY

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Obiokafor, I. N. (2024). Strategies to Mitigate Cyber Identity Theft in Africa's Digital Transformation. *JASSD-Journal of African Studies and Sustainable Development*, *7*(4). https://www.apas.africa/journal_article.php?j=jassd-538

Ogunola, A. A., Sonubi, T., Toromade, R. O., Ajayi, O. O., & Maduakor, A. H. (2024). The intersection of digital safety and financial literacy: Mitigating financial risks in the digital economy. *International Journal of Science and Research Archive*, *13*(02), 673-691. https://www.researchgate.net/profile/Oluwatosin-Ajayi-2/publication/385898197_The_intersection_of_digital_safety_and_financial_literacy_Mitigating_financial_risks_in_the_digital_economy/links/673a8c8b68de5e5a307ef782/The-intersection-of-digital-safety-and-financial-literacy-Mitigating-financial-risks-in-the-digital-economy.pdf

Parsons, K., Butavicius, M., Pattinson, M., & McCormac, A. (2022). Human factors and phishing susceptibility: A systematic review. *Computers & Security, 112*, 102507. https://doi.org/10.1016/j.cose.2021.102507

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? Critique and recommendations. *Research in Nursing & Health, 29*(5), 489–497. https://doi.org/10.1002/nur.20147

Putra, F. P. E., Ubaidi, Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence, 4*(1), 413–421. https://doi.org/10.47709/brilliance.v4i1.4357

Resnik, D. B. (2020). *What is ethics in research and why is it important?* National Institute of Environmental Health Sciences. https://www.niehs.nih.gov/research/resources/bioethics/whatis

Riandari, F., Tasril, V., & Ritonga, R. P. (2024). Increasing cybersecurity awareness among teenagers through digital education and simulation. *Lebah*, *18*(1), 47-55. https://www.plus62.isha.or.id/index.php/abdimas/article/view/269

Rogers R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–177). Guilford Press. https://www.researchgate.net/profile/John_Cacioppo/publication/229068371_Cognitive_and_physiological_processes_in_fear_appeals_and_attitude_change_A_revised_theory_of_protection_motivation/links/54413d630cf2a76a3cc7d17e.pdf

Rosenstock, I. M. (1974). Historical origins of the Health Belief Model. *Health Education Monographs, 2*(4), 328–335. https://doi.org/10.1177/109019817400200403

Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). SAGE.

Sitienei, J. C. (2025). *Evaluating Cybersecurity Threats, Mitigation Measures, and Key Determinants of Security for Kenya's eCitizen Platform* [Doctoral dissertation, Kenyatta University]. https://ir-library.ku.ac.ke/bitstreams/83f72d04-c324-4f53-a08b-9f33c987d8e1/download

Tick, A., & Mai, P. T. (2021). Cybersecurity awareness and behavior of youth in smartphone usage. *Acta Polytechnica Hungarica, 18*(4), 213–230. https://doi.org/10.12700/APH.18.4.2021.4.12

Tolulope, O. J. O. O. (2022). Students' predisposition to being a victim of internet crime in tertiary institutions of Nigeria. *Zamfara Journal of Communication and Contemporary Social Issues, 3*(2), 44–48. https://doi.org/10.26480/ccsj.02.2022.44.48

United Nations Educational, Scientific and Cultural Organization (2023). *Global education monitoring report 2023: Technology in education—A tool on whose terms?* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000385723

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly, 36*(1), 157–178. https://doi.org/10.2307/41410412

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 226-257. https://doi.org/10.63125/fh49az18

World Health Organization. (2011). *Standards and operational guidance for ethics review of health-related research with human participants*. https://apps.who.int/iris/handle/10665/44783

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper & Row.

Zainal, H. Y. (2022). *Examining factors affecting users' cybersecurity behaviour in mobile payment technologies: A hybrid SEM–ANN approach* [Doctoral dissertation, The British University in Dubai]. https://bspace.buid.ac.ae/items/2ee6cd76-2bde-40c0-aaa9-6b74f78c42c2

Zulkiplee, S. M. S., Shukran, M. A. M., Isa, M. R. M., Khairuddin, M. A., Wahab, N., & Hidayat, H. (2025). Examining the impact factors influencing higher education institution (HEI) students' security behaviours in cyberspace environment. *International Journal on Informatics Visualization, 9*(1), 146–152. https://doi.org/10.62527/joiv.9.1.2296

APPENDICES

Appendix I: Consent Form

Title: A Cybersecurity Framework for Mitigating Online Identity Theft and Phishing among Youth in Westlands Constituency, Nairobi County

Principal Investigator

Alice Kemunto Ogoro
Kenya Methodist University
P.O. Box P.O. Box 45240 – 00100

1. Introduction

This Consent Form contains information about the research named above. In order to ensure that you are fully informed about participating in this research, you are requested to read (or have read to you) this form carefully. You will be asked to sign it if you agree to participate. You will also receive a copy for your records. If there is anything you do not understand, please ask for clarification.

2. Reason for the Research

You are being asked to take part in a research study that aims to examine the relationships between technology adoption, cybersecurity education, policy awareness, and the mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County.

3. General Information about the Research

This study is academic in nature and does not involve any medical or experimental procedures. Data will be collected using questionnaires and document review. The research seeks to understand technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing among youth in Westlands Constituency.

4. Your Part in the Research

If you agree to participate, you will be required to:

- Complete a questionnaire
- Provide information about your use of cybersecurity technologies, cybersecurity education and awareness, policy awareness, and experiences and perceptions relating to online identity theft and phishing.

This will take approximately **15–20 minutes**.

Your participation is voluntary.

The study targets 399 respondents aged 18–35 years who have resided in Westlands Constituency for at least one year, have basic digital literacy, and regularly use an internet-enabled device.

5. Possible Risks

There are no physical risks involved in this study.

Possible minimal risks include:

- Discomfort when answering sensitive questions about cyber experiences
- Time inconvenience

You are free to skip any question you do not wish to answer and may stop completing the questionnaire at any time without penalty.

6. Possible Benefits

There may be no direct benefit to you.

However, the study may benefit:

- Youth through improved cybersecurity awareness
- Policymakers through better policy design
- Institutions through enhanced digital safety strategies

7. If You Decide Not to Be in the Research

Participation is completely voluntary. You may choose not to participate without any consequences. Your decision will not affect any services or opportunities available to you.

8. Confidentiality

All information collected will be treated with strict confidentiality.

- You will not be required to provide your name
- Data will be used strictly for academic purposes
- Results will be reported in summary form only
- Only the researcher and supervisors will access the data
- The information collected will be securely stored and handled in a manner that protects the confidentiality of participants.

9. Compensation

You will not receive any payment for participating in this study.

10. Staying in the Research

Participation requires only completion of the questionnaire. There are no additional obligations.

11. Alternatives to Participation

You may choose not to participate and continue with your normal activities.

12. Leaving the Research

You may withdraw from the research at any time without any penalty. You may also decline to answer any question that you are not comfortable answering.

13. If You Have a Problem or Questions

If you have any questions or concerns, please contact:

Researcher:
Alice Kemunto Ogoro

Supervisor:
Dr. Robert Murungi

Kenya Methodist University

14. Your Rights as a Participant

This research will be conducted in accordance with the ethical requirements and approvals applicable to research at Kenya Methodist University.

If you have questions about your rights as a research participant, you may contact the relevant research ethics office through the University.

VOLUNTEER AGREEMENT

The research titled:

"Development of an Integrated Cybersecurity Framework for Mitigating Online Identity Theft and Phishing among Youth in Westlands Constituency, Nairobi County"

has been explained to me. I have read or had the information in this consent form explained to me, have had the opportunity to ask questions, understand that my participation is voluntary and that I may withdraw without penalty, and voluntarily agree to participate in the study.

_____

Date Signature/Mark of Participant

Witness (if applicable)

_____

Date Signature of Witness

Researcher

_____

Date Signature of Researcher

Appendix II: Questionnaire

SECTION A: Demographic Information

Please tick or fill the appropriate response.

1. **Age in Years**

   ☐ 18–22 ☐ 23–27 ☐ 28–31 ☐ 32–35

2. **Gender**:

   ☐ Male ☐ Female ☐ Other / Prefer not to say

3. **Highest level of education**:

   ☐ Secondary ☐ Tertiary (College/TVET)

   ☐ Undergraduate ☐ Postgraduate

4. **Employment status**:

   ☐ Employed ☐ Self-employed ☐ Unemployed ☐ Student

5. **Duration of residence in Westlands**:

   ☐ Less than 1 year ☐ 1–3 years ☐ Over 3 years

6. *How would you describe your daily use of the internet (e.g., work, learning, social media)?*

_____

_____

_____

For section B to F *Please indicate your level of agreement with given statements.* ***Use the Scale: 1 = Strongly Disagree | 2 = Disagree | 3 = Neutral | 4 = Agree | 5 = Strongly Agree***

SECTION B: Technology Adoption

Statement	**1**	**2**	**3**	**4**	**5**
I regularly use antivirus software or firewalls.					
I use strong, unique passwords for my online accounts.					
I have enabled two-factor authentication (2FA) on digital platforms I use.					
I know how to check if a website is secure before sharing personal data.					
I avoid clicking on links or attachments from unknown or suspicious sources.					
I find phishing-detection features in browsers and email platforms easy to use.					

7. *What tools or practices do you use to protect your devices and personal information online?*

SECTION C: Cybersecurity Education

Statement	**1**	**2**	**3**	**4**	**5**
I have received training (formal/informal) on cybersecurity or digital safety.					
I can identify phishing emails or fake digital messages.					
I know where to report cybercrime or phishing attempts.					
I follow cybersecurity tips or updates from trusted sources.					
I feel confident in my ability to avoid identity theft online.					

8. *What kind of cybersecurity training or awareness have you received, and from where?*

SECTION D: Cybercrime Policy Awareness and Perceptions

Statement	**1**	**2**	**3**	**4**	**5**
I am aware of Kenya's cybercrime laws, such as the Computer Misuse and Cybercrimes Act.					
I understand my rights under the Data Protection Act (2019).					
I believe government enforcement of cybercrime policies is effective.					
I believe youth-specific cyber policies are needed in Kenya.					
I trust that authorities will act on reported phishing and identity theft complaints.					

9. *What is your perception of the government's role and effectiveness in preventing cybercrime targeting youth?*

SECTION E: Mitigation of Identity Theft and Phishing

This section assesses the extent to which respondents engage in practices aimed at mitigating online identity theft and phishing. Please indicate the extent to which you agree with each statement.

Scale: 1 = Not Effective | 2 = Slightly Effective | 3 = Neutral | 4 = Effective | 5 = Very Effective

Strategy	**1**	**2**	**3**	**4**	**5**
Cybersecurity training and education programs					
Use of secure tools (2FA, antivirus, spam filters)					
Legal penalties and cybercrime enforcement					
Community-based awareness campaigns					
Tech companies improving platform security					

9. *What do you believe is the most effective way to reduce cybercrime among youth? Why?*

10. *What challenges or barriers do you personally face in protecting your digital identity?*

End of Questionnaire

Thank you for your feedback

Appendix III: Document Review Guide for Secondary Data Collection

No.	Focus Area	Details to Extract	Source Documents	Verification Method	Remarks
1	Reported cases of phishing and identity theft	Reported incidents, affected groups where available, types of incidents and year of report	NCRC reports, CAK/KE-CIRT cybersecurity reports and other relevant official reports	Review and compare information reported in official publications	
2	Cybercrime and data protection policies in place	Name of legislation/policy, year enacted and relevant provisions or objectives	Data Protection Act, 2019; Computer Misuse and Cybercrimes Act, 2018; relevant CAK guidelines	Review official legislation, policies and regulatory documents	
3	Implementation and enforcement mechanisms	Responsible institutions, institutional mandates, reporting mechanisms and documented enforcement measures	Reports and publications from relevant regulatory and government institutions	Compare documented institutional mandates and reported implementation mechanisms	
4	Cybersecurity education and awareness	Nature of cybersecurity education and awareness initiatives, target groups and content areas covered	Government, educational institution and relevant organizational publications	Review documented cybersecurity education and awareness initiatives	
5	Trends and statistics on cybercrime	Reported changes in cyber incidents, common incident types and other relevant cybersecurity trends	CAK/KE-CIRT cybersecurity reports and NCRC publications	Compare reported cybersecurity statistics and trends across the reviewed documents	
6	Youth-focused digital safety initiatives	Nature of initiatives, target groups, coverage where reported and approaches to promoting digital safety	Relevant government, educational institution and organizational publications	Assess documented initiatives in relation to cybersecurity awareness and digital safety among youth	

Appendix IV: Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **955913**

Date of Issue: **22/April/2026**

RESEARCH LICENSE



This is to Certify that Ms.. ALICE KEMUNTO OGORO of Kenya Methodist University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev.2014) in Nairobi on the topic: A CYBERSECURITY FRAMEWORK FOR MITIGATING ONLINE IDENTITY ,THEFT AND PHISHING AMONG YOUTH IN WESTLANDS CONSTITUENCY, NAIROBI COUNTY. for the period ending : 22/April/2027.

License No: **NACOSTI/P/26/4187693**

955913

Applicant Identification Number

Ag. Director General
NATIONAL COMMISSION FOR SCIENCE,TECHNOLOGY & INNOVATION

Verification QR Code

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

See overleaf for conditions