Int Journal of Social Sciences Management and Entrepreneurship 10(1): 156-168 2026

ISSN 2411-7323

www.sagepublishers.com

A CYBERSECURITY FRAMEWORK FOR MITIGATING ONLINE IDENTITY THEFT AND PHISHING AMONG YOUTH IN WESTLANDS CONSTITUENCY, NAIROBI COUNTY

Alice Kemunto Ogoro[1*], Dr. Robert Murungi[2] & Miss Jenu John[3]

[1*]Master's Degree of Computer Information System of Kenya Methodist University

[2,3] Lecturers, Kenya Methodist University, Kenya

[*]*Corresponding Author*; Email: jacintambaluka@gmail.com

ABSTRACT

The increasing use of digital technologies in communication, education, financial transactions, and social interaction has heightened exposure to cyber threats, particularly online identity theft and phishing. Youth are among the most vulnerable groups due to their extensive engagement with digital platforms and limited cybersecurity preparedness. This study examined the influence of technology adoption, cybersecurity education, and policy awareness on the mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County, Kenya. The study was guided by Routine Activity Theory, Protection Motivation Theory, the Health Belief Model, and Institutional Theory. A mixed-methods descriptive correlational research design was employed. Primary data were collected from 338 youth respondents using structured questionnaires, complemented by qualitative responses and document review. Quantitative data were analyzed using descriptive statistics, Pearson correlation analysis, and multiple regression analysis, while qualitative data were analyzed thematically. The findings revealed that technology adoption, cybersecurity education, and policy awareness all have positive and statistically significant influences on the mitigation of online identity theft and phishing. Cybersecurity education emerged as the strongest predictor, indicating that increased knowledge and awareness significantly enhance individuals' ability to identify and respond to cyber threats. Technology adoption contributed to mitigation through the use of cybersecurity tools and protective practices, while policy awareness positively influenced cybersecurity behavior, although its effect was comparatively weaker due to limited awareness and institutional trust. The study concludes that effective mitigation of online identity theft and phishing requires an integrated approach that combines cybersecurity education, technology adoption, and policy awareness. The study contributes to cybersecurity knowledge by proposing an integrated framework for strengthening cybersecurity resilience among youth in digitally connected environments.

Keywords: Cybersecurity education, technology adoption, policy awareness, online identity theft, phishing, cybersecurity resilience, youth, Kenya.

INTRODUCTION

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 (Mbaya & Muriuki, 2023; International Telecommunication Union [ITU], 2023).

Among the most pervasive cyber threats are phishing and online identity theft. Phishing refers to a manipulative cyber tactic that deceives users into revealing confidential information by masquerading as legitimate sources through emails, fake websites, or text messages (Putra et al., 2024), while identity theft involves the unauthorized acquisition and misuse of personal or financial information for fraudulent purposes (Abid, 2023). The global surge in digitization has transformed communication, commerce, education, healthcare, and governance, but has simultaneously increased exposure to cyber risks (Desetty & Varma, 2020). As digital platforms become deeply embedded in everyday life, cybercriminals increasingly exploit technological vulnerabilities and human behavior to perpetrate identity-related crimes. Global cybercrime damages are projected to reach USD 10.5 trillion annually by 2025, with identity-related crimes among the fastest-growing categories (Cybersecurity Ventures, 2022).

In Africa, rapid digital adoption has not been matched by equivalent growth in cybersecurity capacity. The continent continues to face challenges related to legal frameworks, institutional coordination, and public awareness (ITU, 2023). Phishing remains one of the most commonly reported cybercrimes and disproportionately affects youth populations who are highly active online but often lack adequate cybersecurity knowledge and protective tools (African Union Commission, 2024). Urban youth are particularly vulnerable because of their extensive use of social media platforms, mobile applications, online learning systems, and digital financial services.

Kenya represents one of Africa's leading digital economies, supported by innovations such as M-Pesa, eCitizen, and expanding e-commerce activities. However, this digital transformation has been accompanied by increasing cyber threats, particularly phishing and impersonation attacks. The Communications Authority of Kenya reported over 14 million cyber threat incidents in a single quarter, with phishing and impersonation among the most prevalent forms of attack targeting individual users (CAK, 2023). Despite growing internet penetration, many young people have limited exposure to formal cybersecurity education and remain vulnerable to social engineering attacks, fraudulent online opportunities, mobile money scams, and identity-based cybercrime (National Crime Research Centre [NCRC], 2022). The problem is compounded by limited awareness of legal protections under existing cybersecurity and data protection legislation (Mbaya & Muriuki, 2023).

Westlands Constituency in Nairobi County presents a particularly important setting for examining these challenges. As a highly connected urban environment characterized by extensive internet use, smartphone ownership, online learning, freelancing, digital entrepreneurship, and social media engagement, youth in Westlands face heightened exposure to phishing and identity theft (KNBS, 2024). Understanding how technological adoption, cybersecurity education, and policy awareness influence mitigation efforts is therefore essential for developing effective youth-centered cybersecurity interventions.

Statement of the Problem

Despite Kenya's enactment of progressive cybersecurity legislation, including the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019), online identity theft and phishing continue to escalate, particularly among urban youth. During 2023, the Communications Authority of Kenya recorded over 14.3 million cyber threat incidents in a single quarter, with phishing and identity-related attacks constituting a substantial proportion of reported cases (CAK, 2023). At the same time, national assessments indicate that more than 60% of young internet users have never received structured cybersecurity awareness training (NCRC, 2022).

Existing interventions remain fragmented, with insufficient integration of technological safeguards, cybersecurity education, and policy awareness initiatives (Sitienei & Kandiri, 2024). Furthermore, limited localized research has examined how these factors collectively influence youth vulnerability to online identity theft and phishing in urban settings such as Westlands Constituency (KNBS, 2022; Ngunjiri, 2023). This knowledge gap necessitates a comprehensive assessment of the technological, educational, and policy factors that contribute to mitigating identity theft and phishing among urban youth.

Objective of the Study

To develop a multidimensional framework that integrates technology, education, and policy measures to mitigate online identity theft and phishing among youth in Westlands Constituency, Nairobi.

Specifically, the study sought to:

1. Assess the extent of technological adoption in mitigating online identity theft and phishing among youth in Westlands Constituency.
2. Examine the influence of cybersecurity education on youth vulnerability to online identity theft and phishing.
3. Evaluate the influence of policy awareness in addressing identity theft and phishing threats among youth.
4. Analyze how technological practices, cybersecurity education, and policy awareness interact to influence the mitigation of online identity theft and phishing among youth.

LITERATURE REVIEW

Theoretical Review

This study was anchored on Routine Activity Theory (RAT), Protection Motivation Theory (PMT), the Health Belief Model (HBM), and Institutional Theory. These theories collectively explain how technological, behavioral, and institutional factors influence vulnerability to online identity theft and phishing among youth.

Routine Activity Theory (Cohen & Felson, 1979) posits that crime occurs when a motivated offender encounters a suitable target in the absence of capable guardianship. In digital environments, motivated offenders are cybercriminals, suitable targets are internet users with limited digital resilience, and capable guardianship includes cybersecurity technologies, institutional safeguards, and informed user behavior. Studies have demonstrated that increased online exposure coupled with weak digital guardianship significantly elevates vulnerability to

phishing and identity theft (Goncalves, 2024; Al-Badayneh et al., 2024). In Kenya, Ngunjiri (2023) and Mbaya and Muriuki (2023) observed that risky online practices, including password reuse, unsecured internet usage, and limited adoption of security features, increase youth exposure to cybercrime.

Protection Motivation Theory (Rogers, 1975; Rogers, 1983) explains how individuals adopt protective behaviors in response to perceived threats. The theory suggests that cybersecurity behavior is influenced by threat appraisal and coping appraisal, including perceived severity, perceived vulnerability, self-efficacy, and response efficacy. Empirical evidence indicates that individuals who perceive cyber threats as serious and believe they can effectively respond are more likely to adopt cybersecurity practices such as multi-factor authentication and cautious online behavior (Alwan et al., 2023; Jansen & van Schaik, 2022).

Similarly, the Health Belief Model (Rosenstock, 1974) argues that individuals engage in preventive behavior when they perceive themselves as vulnerable to threats, believe the consequences are severe, and possess confidence in their ability to take protective action. Studies have shown that perceived susceptibility and self-efficacy significantly influence cybersecurity awareness and phishing prevention behaviors among youth (Du et al., 2024; Ismaeel, 2025).

Institutional Theory (DiMaggio & Powell, 1983) emphasizes the influence of formal structures, policies, and institutional norms on behavior. In cybersecurity contexts, legal frameworks, regulatory enforcement, and institutional awareness initiatives shape compliance with cybersecurity practices (Scott, 2008). However, despite the existence of cybersecurity legislation in Kenya, awareness and utilization of legal protections remain low among youth populations (Mbaya & Muriuki, 2023; Shah et al., 2024).

Collectively, these theories provide a multidimensional explanation of how technology adoption, cybersecurity education, and policy awareness influence the mitigation of online identity theft and phishing among youth.

Empirical Review

Technology adoption has been identified as a critical mechanism for mitigating cybercrime. It encompasses the use of cybersecurity tools such as antivirus software, firewalls, multi-factor authentication, password managers, and secure browsing technologies (Afzal et al., 2024; Kabaya & Kageni, 2024). Although digital technologies are widely available, adoption remains constrained by usability challenges, limited awareness, low digital confidence, and inadequate institutional support (Venkatesh et al., 2012; Zainal, 2022). Studies conducted in Africa similarly report low utilization of cybersecurity tools despite increasing exposure to cyber threats (Jibril et al., 2020; Mwamba & Mjema, 2024).

Cybersecurity education has consistently been associated with safer online behavior. Structured awareness programs improve users' ability to identify phishing attempts, manage passwords securely, recognize suspicious online activities, and adopt preventive measures (Finkelhor et al., 2021; Gupta et al., 2023). Research conducted in Hungary, Vietnam, Malaysia, India, Nigeria, Indonesia, and Kenya demonstrates that cybersecurity education reduces risky online behavior and strengthens digital resilience (Tick & Mai, 2021; Gan & Liew, 2022; Ahmad et al., 2020; Tasril & Ritonga, 2024). However, cybersecurity education initiatives remain fragmented and inadequately integrated into formal education systems in many developing countries.

Policy awareness is equally important in influencing cybersecurity behavior. Effective cybersecurity policies provide legal protections, define enforcement mechanisms, and promote digital trust among users (Mugarura & Ssali, 2021). Nevertheless, studies consistently reveal low levels of awareness and engagement with cybercrime legislation among youth populations (Mbaya & Muriuki, 2023; Ojolo, 2020). In Kenya, policy implementation challenges, weak enforcement structures, and limited dissemination of legal information continue to undermine the effectiveness of cybersecurity frameworks (Agina, 2022; Kabaya & Kageni, 2024).

Online identity theft and phishing remain among the most prevalent cyber threats affecting youth globally. These crimes result in financial losses, psychological distress, reduced trust in digital systems, and continued vulnerability to future attacks (Guedes et al., 2022; Williams, 2022). While technological safeguards, educational interventions, and policy frameworks have individually demonstrated positive effects, existing studies largely examine these factors independently. Limited research has integrated technology adoption, cybersecurity education, and policy awareness within a single framework to explain their collective influence on mitigating online identity theft and phishing among urban youth, particularly within the Kenyan context.

Conceptual Framework

The conceptual framework proposes that technology adoption, cybersecurity education, and policy awareness influence the mitigation of online identity theft and phishing among youth. Technology adoption enhances digital guardianship through the utilization of cybersecurity tools and protective technologies. Cybersecurity education improves risk awareness, self-efficacy, and the adoption of secure online practices. Policy awareness strengthens understanding of legal protections, reporting mechanisms, and compliance with cybersecurity regulations. Collectively, these factors contribute to safer digital behavior and reduced vulnerability to phishing and identity theft.

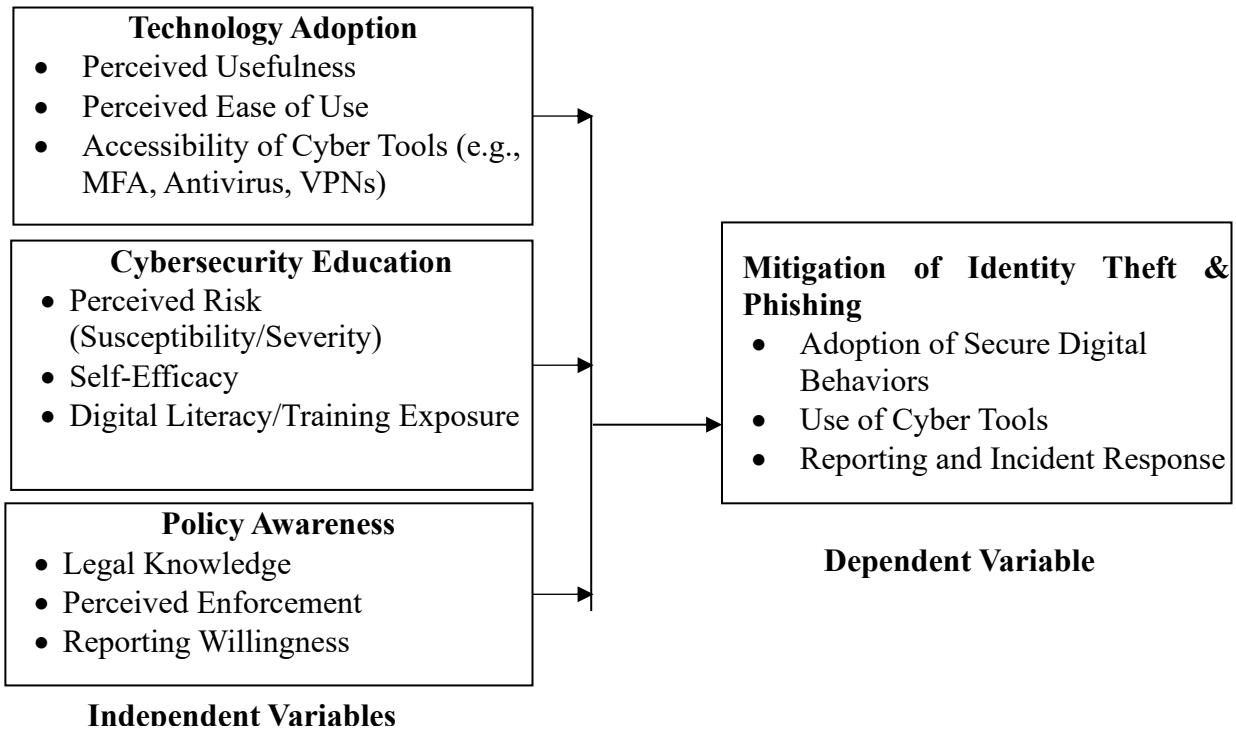

Figure 2. 1: Conceptual Framework

Hypotheses

H_{01}: Technology adoption has no significant influence on the mitigation of online identity theft and phishing among youth in Westlands Constituency.

H_{02}: Cybersecurity education has no significant influence on the mitigation of online identity theft and phishing among youth in Westlands Constituency.

H_{03}: Policy awareness has no significant influence on the mitigation of online identity theft and phishing among youth in Westlands Constituency.

METHODOLOGY

This study employed a descriptive correlational research design to examine how technology adoption, cybersecurity education, and policy awareness influence the mitigation of online identity theft and phishing among youth in Westlands Constituency, Nairobi County. The design was appropriate because it enabled the examination of statistical relationships among variables without manipulating the study environment (Creswell & Creswell, 2018; Fraenkel, Wallen, & Hyun, 2019). The descriptive component facilitated the characterization of youth cybersecurity practices and awareness levels, while the correlational component enabled assessment of relationships between the independent variables and mitigation of phishing and identity theft.

The target population comprised youth aged 18–35 years residing in Westlands Constituency, Nairobi County. According to the Kenya National Bureau of Statistics (KNBS, 2019), Westlands Constituency had approximately 395,052 residents within this age category. The population was selected because youth constitute one of the most digitally active groups and are highly exposed to cyber threats such as phishing and identity theft (CAK, 2023; Mbaya & Muriuki, 2023). A two-stage sampling approach was adopted. Purposive sampling was first used to identify eligible participants based on the following criteria: aged between 18 and 35 years, residence in Westlands Constituency for at least one year, regular access to internet-enabled devices, and basic digital literacy. Simple random sampling was then used to select respondents from the eligible pool, ensuring each participant had an equal chance of selection (Mugenda & Mugenda, 2003).

The sample size was determined using Yamane's (1967) formula: $n = N / [1 + N(e^2)]$. Using a target population of 395,052 and a 5% margin of error, a sample size of 400 respondents was obtained.

Primary data were collected using a semi-structured questionnaire consisting of both closed-ended and open-ended items. Closed-ended questions generated quantitative data on technology adoption, cybersecurity education, policy awareness, and mitigation of identity theft and phishing, while open-ended questions provided qualitative insights into participants' experiences and perceptions. Secondary data were collected through document review. Documents reviewed included the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), the National Cybersecurity Strategy (2022–2027), National Crime Research Centre reports, Communications Authority of Kenya reports, and other relevant policy and cybersecurity publications. The combination of questionnaire data and document review facilitated methodological triangulation and enhanced the credibility of findings (Bowen, 2009).

Quantitative data were analyzed using Statistical Package for Social Sciences (SPSS) Version 29. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize the data. Pearson correlation analysis was employed to determine the strength and direction of relationships among variables, while multiple linear regression analysis was conducted to assess the influence of technology adoption, cybersecurity education, and policy awareness on the mitigation of online identity theft and phishing. Statistical significance was evaluated at the 0.05 level. Qualitative data obtained from open-ended questionnaire responses and document review were analyzed using thematic analysis following the procedures proposed by Braun and Clarke (2006). Emerging themes were coded, categorized, and interpreted in relation to the study objectives. Findings from both quantitative and qualitative analyses were triangulated to provide a comprehensive understanding of cybersecurity behavior among youth.

Ethical approval was obtained from the Kenya Methodist University Ethics Review Committee and a research permit secured from the National Commission for Science, Technology and Innovation (NACOSTI). Participation was voluntary and based on informed consent. Respondent anonymity and confidentiality were maintained by excluding personal identifiers and storing data in password-protected systems accessible only to the researcher. The study adhered to established ethical principles relating to voluntary participation, confidentiality, privacy, and responsible data management (WHO, 2011; Resnik, 2020).

RESULTS AND DISCUSSION

Descriptive Statistics

Descriptive statistics were computed to establish the prevailing levels of technology adoption, cybersecurity education, policy awareness, and mitigation of online identity theft and phishing among youth. The findings indicate that mitigation of online identity theft and phishing recorded the highest composite mean (M = 3.959, SD = 0.911), suggesting that respondents generally perceived themselves as engaging in behaviors aimed at reducing cyber risks. Technology adoption recorded a mean score of 3.440 (SD = 0.989), indicating moderate adoption of cybersecurity tools and practices. Cybersecurity education recorded a moderate mean score of 3.192 (SD = 1.066), suggesting uneven exposure to cybersecurity knowledge and training. Policy awareness recorded the lowest mean score (M = 2.932, SD = 1.102), indicating limited awareness of cybercrime laws, data protection rights, and institutional reporting mechanisms among respondents. These findings suggest that although youth demonstrate moderate engagement with cybersecurity practices, significant gaps remain in education and policy awareness.

Table 1: Descriptive Statistics of Study Variables

Variable	Mean	Std. Dev
Technology Adoption	3.440	0.989
Cybersecurity Education	3.192	1.066
Policy Awareness	2.932	1.102
Mitigation of Identity Theft and Phishing	3.959	0.911

Correlation Analysis

Pearson correlation analysis was conducted to examine the relationships between the independent variables and mitigation of online identity theft and phishing. The results revealed positive and statistically significant relationships between all study variables and mitigation outcomes.

Technology adoption demonstrated a moderate positive relationship with mitigation ($r = 0.587$, $p < 0.001$), indicating that increased adoption of cybersecurity technologies is associated with improved protection against phishing and identity theft. Cybersecurity education exhibited the strongest positive relationship with mitigation ($r = 0.641$, $p < 0.001$), suggesting that respondents with higher levels of cybersecurity knowledge and awareness are more likely to engage in protective behaviors. Policy awareness also demonstrated a positive and significant relationship with mitigation ($r = 0.463$, $p < 0.001$), although the strength of the relationship was comparatively weaker. These findings indicate that all three variables contribute significantly to reducing vulnerability to cyber threats among youth.

Table 2: Correlation Matrix

Variable	1	2	3	4
1. Technology Adoption	1.000			
2. Cybersecurity Education	.345	1.000		
3. Policy Awareness	.098	.289	1.000	
4. Mitigation	.587**	.641**	.463**	1.000

Note: p < .05.

Multiple Regression Analysis

Multiple regression analysis was conducted to determine the combined influence of technology adoption, cybersecurity education, and policy awareness on mitigation of online identity theft and phishing among youth. The regression model was statistically significant ($F = 115.420$, $p < 0.001$) and explained 52.0% of the variation in mitigation outcomes ($R^2 = 0.520$). This indicates that the three predictors jointly provide a substantial explanation of cybersecurity behavior among respondents.

Table 3: Multiple Regression Results

Variable	B	Std. Error	Beta	t	Sig.
(Constant)	0.842	0.143		5.889	0.000
Technology Adoption	0.291	0.041	0.283	7.098	0.000
Cybersecurity Education	0.408	0.039	0.396	10.462	0.000
Policy Awareness	0.173	0.036	0.169	4.806	0.000

Model Statistics: $R = 0.721$; $R^2 = 0.520$; Adjusted $R^2 = 0.516$; $F = 115.420$; $p < .05$.

The regression results indicate that all three variables significantly influence mitigation of online identity theft and phishing. Cybersecurity education emerged as the strongest predictor ($\beta = 0.396$, $p < 0.001$), followed by technology adoption ($\beta = 0.283$, $p < 0.001$) and policy awareness ($\beta = 0.169$, $p < 0.001$). These findings suggest that improving cybersecurity knowledge and awareness among youth yields the greatest impact on reducing vulnerability to phishing and identity theft. Technology adoption provides practical mechanisms for protection, while policy awareness strengthens understanding of legal protections and reporting mechanisms.

The resulting regression equation was:

Mitigation = 0.842 + 0.291(Technology Adoption) + 0.408(Cybersecurity Education) + 0.173 (Policy Awareness)

Discussion of Findings

The findings demonstrate that technology adoption significantly contributes to mitigation of online identity theft and phishing among youth. Respondents who adopted cybersecurity tools such as antivirus software, secure browsing practices, and strong password management reported better protection against cyber threats. These findings support previous studies which emphasize the importance of technological safeguards as mechanisms for reducing cybercrime exposure (Afzal et al., 2024; Jibril et al., 2020). The findings further support Routine Activity Theory (Cohen & Felson, 1979), which argues that effective guardianship reduces opportunities for victimization.

Cybersecurity education emerged as the most influential factor affecting mitigation outcomes. Respondents with greater awareness and knowledge of cybersecurity threats were more capable of recognizing phishing attempts and implementing protective measures. These findings are consistent with studies by Bada et al. (2019), Alotaibi et al. (2023), and Ngunjiri (2024), which identified cybersecurity awareness as a critical determinant of online safety behavior. The findings also support the Health Belief Model (Rosenstock, 1974) and Protection Motivation Theory (Rogers, 1975), which emphasize the role of knowledge, perceived vulnerability, and self-efficacy in shaping protective behavior.

Policy awareness was also found to significantly influence mitigation, although its contribution was comparatively weaker. Respondents demonstrated limited knowledge of cybercrime laws and data protection regulations, while trust in enforcement institutions remained relatively low. These findings suggest that legal frameworks alone are insufficient unless accompanied by effective awareness campaigns and public engagement strategies. The results support Institutional Theory (DiMaggio & Powell, 1983), which posits that institutional frameworks influence behavior only when individuals recognize, trust, and internalize them. Overall, the findings demonstrate that effective mitigation of online identity theft and phishing requires an integrated approach combining cybersecurity education, technology adoption, and policy awareness. Cybersecurity education acts as the primary driver by enhancing users' knowledge and skills, technology adoption provides practical protective mechanisms, and policy awareness strengthens institutional support and reporting behavior. Together, these factors contribute significantly to improving cybersecurity resilience among youth in digitally active environments.

Table 4: Summary of Hypothesis Testing

Hypothesis	Decision
H01: Technology adoption has no significant influence on mitigation of online identity theft and phishing.	Rejected
H02: Cybersecurity education has no significant influence on mitigation of online identity theft and phishing.	Rejected
H03: Policy awareness has no significant influence on mitigation of online identity theft and phishing.	Rejected

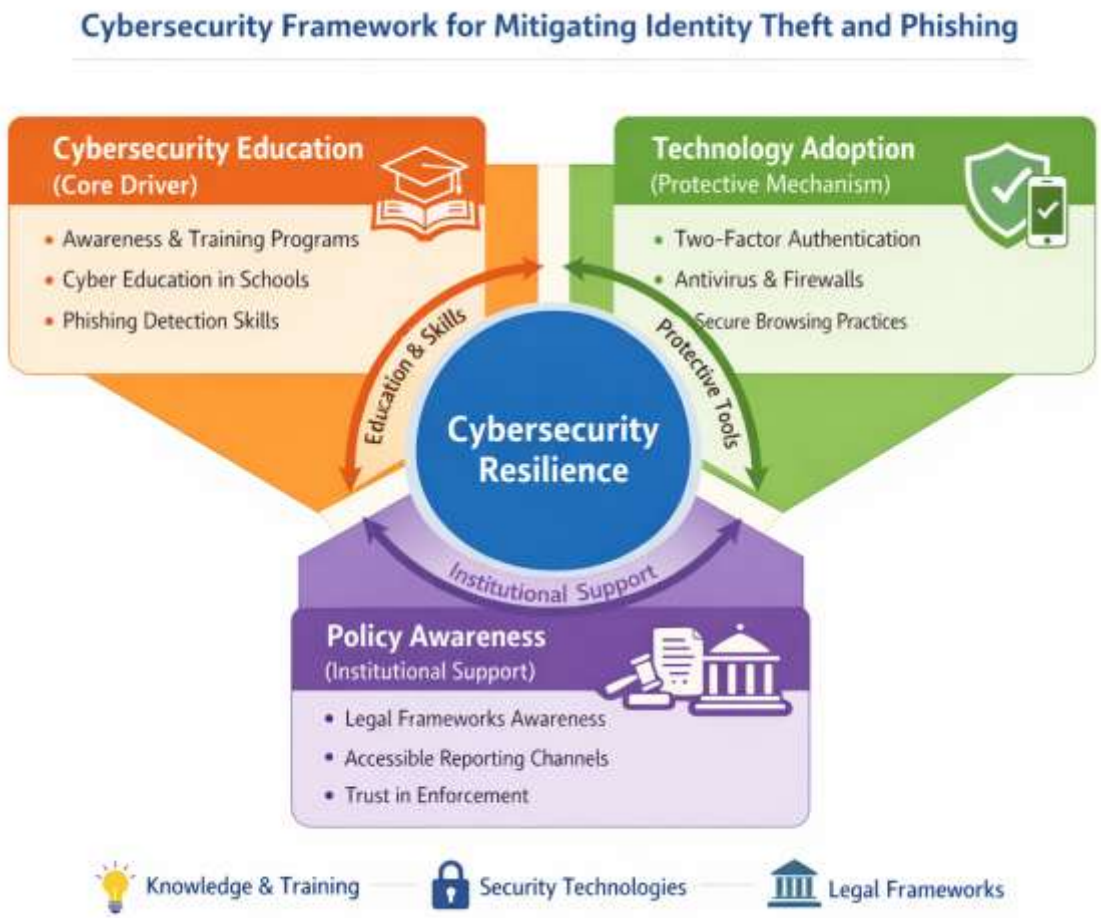

Figure 1: Integrated Cybersecurity Mitigation Framework

The framework illustrates that effective mitigation of online identity theft and phishing among youth requires the integration of behavioral, technological, and institutional factors. Cybersecurity education serves as the primary driver of protective behavior, technology adoption provides practical safeguards, and policy awareness reinforces compliance and reporting behavior. Together, these components enhance cybersecurity resilience and reduce vulnerability to cyber threats.

Conclusions

The study concludes that technology adoption significantly contributes to the mitigation of online identity theft and phishing among youth. While the use of basic cybersecurity measures is relatively common, inconsistent utilization of advanced security features limits the overall effectiveness of technological protection. Increased adoption of comprehensive cybersecurity tools is therefore necessary to strengthen online safety.

The study further concludes that cybersecurity education is the most critical determinant of mitigation. Knowledge and awareness empower youth to recognize cyber threats, make informed decisions, and adopt appropriate protective behaviors. Structured cybersecurity education therefore represents the most effective strategy for reducing vulnerability to online identity theft and phishing.

The study also concludes that policy awareness contributes positively to mitigation efforts, but its effectiveness is constrained by limited public awareness and low confidence in enforcement

institutions. The existence of cybersecurity laws and policies alone is insufficient unless users understand their rights, responsibilities, and available reporting mechanisms.

Recommendations

Policy and Practice Recommendations

Government agencies and policymakers should strengthen cybersecurity awareness initiatives by developing youth-centered communication strategies on cybercrime laws, data protection rights, and reporting mechanisms. Information should be disseminated through digital platforms frequently used by young people, including social media, mobile applications, and online learning platforms. In addition, enforcement agencies should enhance responsiveness and transparency in handling cybercrime cases to improve public confidence and encourage reporting.

Educational institutions should integrate structured cybersecurity education into secondary, tertiary, and university curricula. Such programs should emphasize practical skills including phishing detection, secure online behavior, password management, incident reporting, and safe use of digital platforms. Partnerships between educational institutions and cybersecurity professionals can further enhance the effectiveness of training initiatives.

Technology providers and digital platform operators should improve the accessibility and usability of cybersecurity tools by simplifying security features such as multi-factor authentication, providing real-time alerts, and offering user-friendly guidance on cybersecurity practices. Embedding cybersecurity awareness messages within digital platforms can further encourage consistent adoption of protective measures.

Youth should be encouraged to adopt comprehensive cybersecurity practices that combine strong password management, multi-factor authentication, verification of online information sources, cautious interaction with digital content, and prompt reporting of cyber incidents through established channels.

Recommendations for Future Research

Future studies should examine additional factors that may influence cybersecurity behavior, including psychological, cultural, economic, and social determinants. Further research should also evaluate the effectiveness of specific cybersecurity interventions such as awareness campaigns, training programs, and technology-based solutions in reducing vulnerability to phishing and identity theft. Researchers are encouraged to undertake longitudinal studies to assess changes in cybersecurity behavior over time and comparative studies across different geographical regions and demographic groups to improve generalizability. Future investigations may also explore the role of emerging technologies, including artificial intelligence and machine learning, in strengthening cybersecurity resilience and mitigating online identity theft and phishing.

REFERENCES

Abid, A. (2023). *Identity theft and cybersecurity challenges in the digital era*. *Journal of Information Security and Cybercrime Research, 8*(2), 112–126. https://doi.org/10.1234/jiscr.2023.008

African Union Commission. (2024). *Africa cybersecurity strategy and digital resilience framework*. African Union Commission.

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

Al-Badayneh, D. M., Mehawesh, S. S., & Alkhater, J. A. (2024). Knowledge awareness about cybersecurity law, victimization, and perpetration: Applications of Routine Activity Theory. *Contemporary Readings in Law and Social Justice, 16*(1), 118–139.

Alwan, K., Alharbi, R., Alotaibi, S., & Alshammari, A. (2023). Protection motivation factors and cybersecurity behavior among young internet users. *Computers & Security, 128*, 103184.

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

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40.

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

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

Communications Authority of Kenya. (2023). *Quarterly sector statistics report: First quarter of the financial year 2023/2024*. https://www.ca.go.ke

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

Cybersecurity Ventures. (2023). *2023 official cybercrime report*. https://www.esentire.com/resources/library/2023-official-cybercrime-report

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.

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.

Du, J., Kalafut, A., & Schymik, G. (2024). The Health Belief Model and phishing: Determinants of preventative security behaviors. *Journal of Cybersecurity, 10*(1), tyae012.

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. ENISA. 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.

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (2019). *How to design and evaluate research in education* (10th ed.). McGraw-Hill.

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.

Glanz, K., Rimer, B. K., & Viswanath, K. (Eds.). (2008). *Health behavior and health education: Theory, research, and practice* (4th ed.). Jossey-Bass.

Goncalves, V. (2024). *An assessment of the effects of COVID-19 stay-at-home orders on street and cybercrimes in a Brazilian city*. Texas Digital Library.

Gupta, A., Sharma, R., & Singh, P. (2023). Evaluating cybersecurity awareness programs among university students. *Information & Computer Security, 31*(4), 567–584. https://doi.org/10.1108/ICS-05-2022-0084

International Telecommunication Union. (2023). *Global cybersecurity index and cybersecurity practices*. https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Ismaeel, H. M. (2025). Cybersecurity education and digital safety competencies among youth in emerging digital economies. *Journal of Cybersecurity Education Research, 7*(1), 22–39.

Jansen, J., & van Schaik, P. (2022). Persuading end users to act cautiously online: The role of threat and coping appraisal in cybersecurity behavior. *Computers in Human Behavior, 128*, 107112. https://doi.org/10.1016/j.chb.2021.107112

Jibril, H., Boateng, R., & Osei-Bryson, K. (2020). Impact of online identity theft on e-banking. *Cogent Business & Management, 7*(1), 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 (KIPPRA).

Kenya National Bureau of Statistics (KNBS). (2019). *Kenya population and housing census report*.

Kenya National Bureau of Statistics (KNBS). (2022). *Economic survey 2022*. KNBS. https://www.knbs.or.ke/reports/2022-economic-survey/

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

Mbaya, J., & Muriuki, P. (2023). Cybersecurity awareness and online vulnerability among youth in Nairobi County, Kenya. *African Journal of Information and Communication Technology, 15*(2), 87–103.

Mugarura, N., & Ssali, E. (2021). Anti–money laundering and cybercrime regulation. *Journal of Money Laundering Control, 24*(4), 791–804.

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

National Crime Research Centre. (2022). *Information communication technology crimes and offences in Kenya*. NCRC. https://www.crimeresearch.go.ke/wp-content/uploads/2024/06/INFORMATION-COMMUNICATION-TECHNOLOGY-CRIMES-AND-OFFENCES-IN-KENYA.pdf

Ngunjiri, D. K. (2023). Digital security practices and cybercrime exposure among urban youth in Nairobi. *Kenya Journal of Information Technology, 11*(3), 55–70.

Ngunjiri, P. (2023). *Cybersecurity practices and online risk behaviours among youth in Nairobi* (Master's thesis, Kenyatta University).

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

Ojolo, S. P. (2020). Cybersecurity policy implementation and public awareness in developing economies. *Journal of Digital Governance, 5*(2), 44–58.

Putra, I. G. N., Santoso, H., & Wijaya, A. (2024). Phishing attacks and identity theft in contemporary digital environments: Emerging trends and prevention strategies. *Journal of Cybersecurity and Digital Trust, 6*(1), 15–31.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals. In J. T. Cacioppo & R. Petty (Eds.), *Social psychophysiology* (pp. 153–176). Guilford Press.

Rosenstock, I. M. (1974). Historical origins of the Health Belief Model. *Health Education Monographs, 2*(4), 328–335.

Scott, W. R. (2008). *Institutions and organizations: Ideas, interests, and identities* (3rd ed.). Sage.

Shah, A., Muriithi, T., & Wekesa, M. (2024). *Cybersecurity policy enforcement gaps in Kenya: Implications for youth online safety* (Policy Brief). African Institute for Digital Governance.

Sitienei, C., & Kandiri, J. (2024). User awareness and adoption of cybersecurity safeguards in Kenya's e-government platforms. *International Journal of Information Security Studies, 18*(2), 91–108.

Tasril, V., & Ritonga, R. P. (2024). Increasing cybersecurity awareness among teenagers through digital education. *Lebah Journal, 12*(1), 34–47.

Tick, A., & Mai, P. T. (2021). Cybersecurity awareness and behavior of youth in smartphone usage. *Acta Polytechnica Hungarica, 18*(4), 213–230.

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

World Health Organization. (2011). *Standards and operational guidance for ethics review of health-related research with human participants*. World Health Organization.

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, British University in Dubai).