

Social Media Behavior and Cybersecurity Threats Among University Students in Uganda

Mackenzie Deborah Kaddu¹; Sam Njumwamukama²

¹Lecturer, Victoria University, Kampala

²Makerere University

Publication Date: 2026/09/30

Abstract

The widespread use of social media among university students has created new opportunities for communication and learning, but it has also increased exposure to cybersecurity threats. This study examined how students' social media behavior influences their vulnerability to cyber risks in higher education institutions in Uganda. The research focused on students from Victoria University, Ndejje University, and YMCA Vocational Institute. A cross-sectional mixed-methods approach was used, combining quantitative survey data with qualitative interviews to capture both patterns of behavior and students' experiences with online risks. Quantitative data were analyzed using descriptive statistics, correlation, and chi-square tests, while qualitative responses were examined through thematic analysis. The findings indicate that common practices such as sharing personal information online, reusing passwords, accepting unknown friend requests, and clicking unverified links significantly increase students' exposure to threats such as phishing, identity theft, and account compromise. The study also found gaps in cybersecurity awareness and limited institutional guidance on safe online practices. These results highlight the need for universities to strengthen digital safety education and integrate cybersecurity awareness into student training and orientation programs. Enhancing students' understanding of safe social media use can reduce vulnerability and support a more secure digital environment within higher education institutions.

Keywords: Social Media Behavior, Cybersecurity Threats, University Students.

I. INTRODUCTION

➤ Introduction

In the digital age, social media has changed how people communicate, collaborate, and learn. Among university students, platforms such as Facebook, WhatsApp, Instagram, and TikTok became central to academic, social, and entertainment activities. However, this unprecedented connectivity came with increasing vulnerability to cyber threats, including phishing, identity theft, malware, and social engineering attacks. The youthful demographic, while digitally native, often lacked the necessary cybersecurity awareness to safeguard themselves effectively [1]. Globally, university students were among the most active users of social media, but they also represented a disproportionately high percentage of cybercrime victims due to risky behaviors such as oversharing, password reuse, and clicking on suspicious links [2]. The education sector, particularly in developing regions, remained under-protected despite being highly targeted by cyber attackers. In Uganda, limited empirical data existed on how student behaviors on social media

contributed to their exposure to cyber risks. This study therefore investigated the influence of social media behavior on cybersecurity threats among students at Victoria University, Ndejje University, and YMCA Vocational Institute, aiming to bridge a critical knowledge gap and guide targeted cybersecurity education.

➤ Background of the Study

The rapid digitization of education made social media platforms indispensable to students globally. As of 2023, over 4.9 billion people were active on social media, with young adults (ages 18–29) constituting the largest demographic [3]. Simultaneously, cybercrime surged, costing the global economy an estimated \$10.5 trillion annually by 2025 [4]. University students, while tech-savvy, often lacked sufficient awareness of basic digital safety practices [5], and their behaviors like sharing passwords or location data made them attractive targets for cybercriminals. Across Africa, social media penetration grew significantly, particularly among youth populations. However, cybersecurity infrastructure and education lagged behind. Reports by [6] and the African

Union indicated that education institutions were among the top five targets of cyberattacks on the continent. A study conducted in Nigeria found that 64% of university students were unaware of the consequences of clicking malicious links on social media [7]. Despite government investments in national cybersecurity frameworks, implementation at educational institutions remained inadequate.

In East Africa, Kenya, Rwanda, and Tanzania launched national digital literacy campaigns, yet cybersecurity training rarely reached university campuses [8]. Social media misuse, particularly among students, led to increased incidents of account hacking, impersonation, and online fraud. The East African Communications Organisation (EACO) emphasized in its 2023 report the urgent need for member countries to develop targeted cybersecurity awareness initiatives for university students. Uganda's internet penetration stood at 52% as of 2023, with social media being the dominant form of online activity among young people [9]. University students, especially in urban centers, were daily users of multiple platforms. The Uganda National Computer Emergency Response Team (CERT-UG) reported a 36% increase in student-related cybercrime incidents between 2021 and 2023, including phishing, online scams, and credential theft [10]. Despite this, cybersecurity education was not systematically integrated into higher education curricula, and institutions lacked dedicated awareness programs tailored to student behaviors.

Victoria University, Ndejje University, and YMCA Vocational Institute represented diverse higher learning environments in Uganda—private, public, and vocational respectively. While each institution had basic ICT policies, none had institution-wide, behavior-focused cybersecurity programs. This made their students both digitally engaged and relatively unprotected, presenting a critical gap that this study sought to address.

➤ *Problem Statement*

The widespread use of social media among university students in Uganda presented an increasingly complex cybersecurity challenge. Platforms such as WhatsApp, Facebook, Instagram, TikTok, and Telegram were widely adopted by students for academic communication, personal branding, and social interaction [11]. However, this online presence created fertile ground for cybercriminal activity, with social platforms becoming primary vectors for phishing, identity theft, social engineering, and malware distribution ([12], [1]). Students frequently engaged in risky digital practices such as oversharing personal information, using weak or repeated passwords, ignoring privacy settings, and clicking suspicious links—behaviors that were strongly associated with increased exposure to cyber threats ([8], [2]). Across sub-Saharan Africa, a growing body of evidence indicated that university students were highly susceptible to digital exploitation. For instance, a regional study by [12] found that 67% of university students in South Africa had experienced phishing or social media impersonation, while over 45% reused passwords across

accounts. In Uganda, a nationwide survey by [9] indicated that over 60% of cybercrime victims under the age of 30 were students or young adults, with credential theft and online impersonation ranking among the top reported attacks.

More concerning was the evident lack of preventative knowledge and institutional preparedness. [8] revealed that only 24% of students surveyed in East Africa had received formal cybersecurity training, and less than 20% were aware of multi-factor authentication protocols. Despite government initiatives from bodies like the National Information Technology Authority–Uganda (NITA-U) and the National CERT (CERT-UG), interventions remained mostly infrastructure-focused, with minimal emphasis on behavioral vulnerabilities at the student level ([10], [13]). Compounding the issue was the absence of behaviorally-focused empirical research within the Ugandan higher education context. Most studies had either emphasized access to digital infrastructure or general digital literacy, failing to examine how specific online behaviors—such as public profile exposure, interaction with unknown contacts, or ignorance of security tools—correlated with real-world cyber incidents. Consequently, a significant knowledge gap existed in understanding how individual behavioral tendencies on social media contributed to vulnerability, and what protective strategies could be behaviorally targeted to reduce exposure.

This study filled that gap by empirically investigating the specific risky social media behaviors exhibited by university students in Uganda and their statistical correlation with the types and frequency of cybersecurity threats experienced. By identifying these behavioral triggers, the research aimed to support the development of targeted institutional interventions, digital safety programs, and policy recommendations that were contextualized to the Ugandan student population and aligned with global best practices.

➤ *General Objective*

The general objective of this study was to investigate the relationship between social media behavior and exposure to cybersecurity threats among students in selected higher learning institutions in Uganda.

➤ *Specific Objectives*

The study was guided by the following specific objectives:

- To identify the most commonly used social media platforms by students.
- To assess the prevalence of risky social media behaviors (e.g., oversharing, poor password practices).
- To determine the types and frequency of cybersecurity threats experienced by students.
- To evaluate students' awareness and understanding of cybersecurity risks on social platforms.

➤ *Justification*

The urgency of this study was rooted in the escalating cybersecurity threat landscape, especially as it related to higher learning institutions in Uganda. As digital technologies increasingly became intertwined with student life, it was imperative to address the behavioral dimensions of cybersecurity risk. Despite national initiatives by NITA-U and CERT-UG, students continued to engage in unsafe online practices, making them soft targets for cybercriminals. The gap between digital engagement and cybersecurity awareness was not just a knowledge issue—it was a behavioral issue that required targeted inquiry and intervention.

This study provided a novel contribution by focusing specifically on the behavioral predictors of cyber threat exposure, a domain often neglected in traditional ICT risk assessments. Its findings offered actionable insights for universities, regulators, and digital rights advocates in Uganda. Furthermore, the study served as a baseline for developing behavior-focused cybersecurity awareness curricula, contributed to risk reduction policies, and helped align institutional practices with the unique threat profiles of young, digitally active populations.

➤ *Scope of the Study*

• *Geographical Scope:*

This study was geographically situated within Uganda, targeting three higher learning institutions with distinct characteristics to ensure contextual diversity and relevance. These institutions were Victoria University, a private urban-based university; Ndejje University, which operated both urban and rural campuses; and YMCA Vocational Institute, a semi-professional institution offering vocational and technical education in Kampala. These institutions represented a mix of academic, technological, and socio-economic settings, enabling the study to capture a holistic view of student social media behavior and associated cybersecurity threats.

• *Conceptual Scope:*

The conceptual scope of the study was centered on understanding the relationship between student behavior on social media platforms and their exposure to cybersecurity threats. Specifically, it investigated the platforms used, the nature of behavioral risks (e.g., oversharing, password reuse, risky clicks), types of threats encountered (phishing, identity theft, impersonation), and students' awareness and preventive behaviors. It did not focus on technical infrastructural vulnerabilities, firewalls, or institutional security systems, but rather on user-centered risks and habits.

• *Time Scope:*

This study was conducted within a one-month timeframe, aligning with practical research timelines and academic schedules. Data collection targeted recent experiences, with participants reflecting on incidents or behaviors from the preceding 12 months. This short-term study approach was sufficient for collecting rich, behavior-focused data, particularly through surveys.

II. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

➤ *Introduction*

This chapter presented a review of existing literature on social media behavior and cybersecurity threats among university students. The literature was organized around the five key research objectives, and the theoretical framework underpinning the study was discussed in detail.

➤ *Theoretical Framework: Protection Motivation Theory (PMT)*

The study was underpinned by Protection Motivation Theory (PMT) developed by [14] and later expanded in health and cybersecurity psychology. PMT explained how individuals were motivated to adopt protective behaviors in response to perceived threats. It posited that when confronted with a risky situation (like potential cyberattacks), individuals evaluated:

- Perceived severity: How serious the threat was (e.g., data loss or account theft)
- Perceived vulnerability: Their likelihood of being affected
- Response efficacy: Belief that available protective measures (e.g., using 2FA) were effective
- Self-efficacy: Confidence in their ability to adopt such measures

PMT was suitable for this study because cybersecurity, like health, required preventive action influenced by perceptions and motivation, not just technical knowledge. In the university context, students' decisions to protect themselves online depended on how serious they believed cyber risks were, whether they saw themselves as targets, and whether they felt capable of taking action. PMT had been widely applied in digital behavior research and was a strong fit for explaining why some students practiced cyber hygiene while others did not ([8], [1]).

➤ *Conceptual Framework*

Building upon the Protection Motivation Theory (PMT), the conceptual framework for this study identified three critical variable groups—-independent variables, moderating variables, and dependent variables—each playing a distinct role in shaping students' cybersecurity outcomes within the context of social media use.

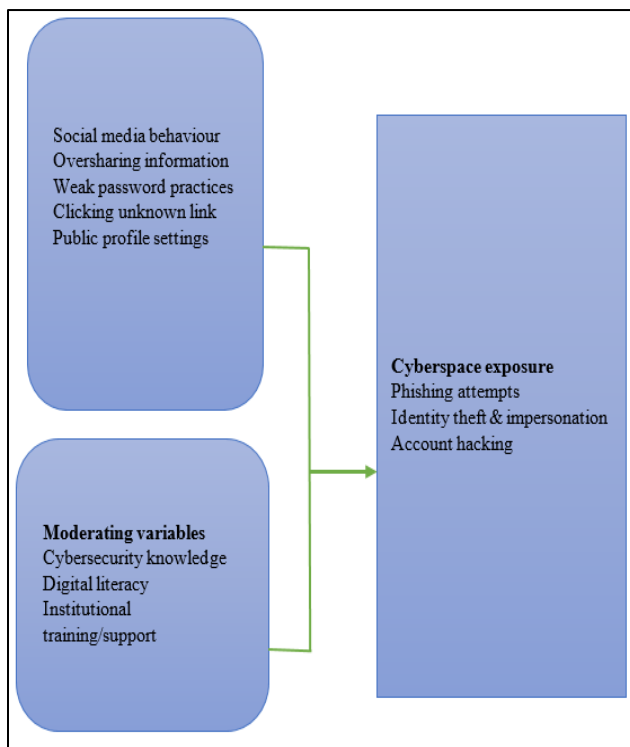


Fig 1 Conceptual Framework

At the core of the framework were the independent variables, which captured specific social media behaviors exhibited by university students. These included: The tendency to overshare personal information (such as photos, contact details, and real-time location), The use of weak or recycled passwords, The habitual clicking on suspicious or unverified links, maintaining public or unprotected social media profiles, frequently interacting with unknown or unverified online contacts. These behaviours were widely recognized in the literature as significant risk vectors for cybersecurity incidents, particularly among youth and university-age populations ([8], [1]).

The impact of these behaviors did not occur in isolation. The relationship between risky actions and cybersecurity threat exposure was shaped by a set of moderating variables, which either intensified or reduced the likelihood of harm. These included: Students' levels of cybersecurity awareness (e.g., knowledge of phishing or identity theft), Digital literacy (ability to use digital tools securely), The influence of peer norms (social pressure or trends that normalized risky behavior such as location tagging or public posting), Prior experience with cyber incidents & Institutional interventions such as formal digital safety training or access to online security resources. These moderators aligned closely with PMT's constructs of perceived vulnerability, coping efficacy, and response mechanisms.

- *Dependent Variables:*

The dependent variables represented the outcomes of interest that the study sought to understand and measure. These fell into two broad categories:

- *Exposure to Cybersecurity Threats:*

Phishing attacks, Unauthorized access or hacking of accounts, Social media impersonation, Credential theft & Malware infections resulting from social media interactions.

- *Adoption of Protective Behaviors:*

Enabling two-factor authentication (2FA), Restricting public access to social profiles, Regularly updating passwords, Proactively reporting or blocking suspicious activity.

Together, this framework provided a comprehensive structure to investigate how specific behaviors on social platforms—moderated by awareness and digital skills—affected the vulnerability or resilience of university students to cyber threats. It created a pathway for empirical testing and supported the development of targeted behavioral interventions that went beyond technical infrastructure, addressing the human dimension of cybersecurity in the higher education context.

➤ *Review of Literature*

- *Identifying the Most Commonly Used Social Media Platforms by Students:*

Extant literature consistently established social media as integral to university students' daily routines. Globally, WhatsApp, Instagram, TikTok, and Facebook dominated in terms of frequency and functionality [2]. These platforms were favored for their accessibility, real-time communication features, and integration with academic life. In the African context, [7] and [12] confirmed similar patterns, showing WhatsApp as the primary communication tool for students in Nigeria and South Africa, respectively.

In Uganda, the [9] reported that WhatsApp usage among youth aged 18–30 (a proxy demographic for university students) exceeded 90%. Additionally, TikTok and Instagram saw exponential growth, particularly in urban areas. However, these studies focused on usage trends without linking them to security vulnerabilities, especially in higher education contexts. What remained under-researched was how the affordances of these platforms (such as public sharing and open messaging) related to actual cyber threat exposure. The existing research identified commonly used platforms but rarely explored their associated threat surfaces in educational environments. This study bridged that gap by contextualizing platform use in relation to behavioral risks.

- *Assessing the Prevalence of Risky Social Media Behaviours:*

A considerable volume of global literature highlighted risky social media behaviors among students—such as oversharing personal details, using weak passwords, and accepting requests from strangers [1]. These behaviors were not merely casual; they constituted digital risk factors that increased susceptibility to cyber threats. [8] emphasized that students often failed

to understand how casual online behaviors translated into security breaches.

In Africa, [7] found that over 50% of university students admitted to reusing passwords and engaging in unsafe link-sharing practices. Similarly, in South Africa, simulated phishing tests showed that students were easily deceived by social media-styled attacks [12]. However, empirical data on these behaviors within Ugandan universities remained limited. While anecdotal evidence and small institutional surveys existed (e.g., [15]), comprehensive behavioral assessments linked to platform features were rare. The prevalence and typologies of risky social media behavior were well-documented globally, but local data was lacking, especially studies that quantified specific behaviors and linked them to actual threats.

This study contributed novel data in that domain by quantifying risky behaviors and examining their relationship to threat exposure in the Ugandan context.

- *Determining the Types and Frequency of Cybersecurity Threats Experienced:*

Cyber threats facing students predominantly included phishing, account hijacking, and identity theft. Global studies consistently showed that social media platforms were key attack vectors. [2] reported that 68% of students encountered phishing attempts via social media direct messages, while [8] observed high impersonation rates among students with public-facing profiles. In Uganda, the [13] report confirmed a 36% increase in education-related cyber incidents, with phishing and social engineering attacks leading. However, these statistics were aggregate-level and lacked segmentation by demographic (e.g., students versus staff). Similarly, institutional data from universities like Makerere and KIU were fragmented and mostly qualitative.

- ✓ *Gap Identified:*

While threat types were broadly identified, there was little quantification of their frequency or severity among university students in Uganda. This study empirically measured the frequency and nature of cyber incidents directly linked to student behavior on social media.

- *Evaluating Students' Awareness and Understanding of Cybersecurity Risks:*

Although digital literacy was increasing, cybersecurity-specific knowledge remained deficient. Globally, [1] found that only 23% of students understood what constituted a phishing attempt. In East Africa, [7] found a similar trend: general awareness was high, but behavior-specific cybersecurity knowledge was remarkably low. In Uganda, the study by [15] at Makerere University reported that only 19% of students could identify a fraudulent login page. While ICT skills may have been improving, awareness of how behaviors influenced vulnerability was still missing. Institutional interventions, where they existed, tended to be technical or policy-based rather than behavioral.

- ✓ *Gap Identified:*

Existing studies identified knowledge gaps, but few investigated the disconnect between what students knew and what they did—a core issue this study investigated using PMT to map behavior against awareness levels.

- *Examining the Correlation between Behavior and Cyber Threat Exposure:*

The final dimension of this review synthesized studies that linked risky behavior to actual cyber incidents. Globally, there was consensus on this relationship. [1] used structural equation modelling to demonstrate that students who engaged in high-risk behaviors were significantly more likely to experience phishing or account compromise. [8] also showed 2.4 times increase in threat exposure among students who overshared or ignored privacy settings. However, most of these studies were set in developed countries or regions with structured cybersecurity ecosystems. Very few focused on students in under-resourced institutional contexts, where infrastructure was weak and policies may not have existed. In Uganda, empirical data correlating behaviors to threats remained anecdotal.

No current Ugandan study had empirically tested the statistical relationship between social media behaviors and threat exposure. This research filled that gap using survey-based correlation and regression analysis, establishing causal insights for education policy and institutional intervention.

III. METHODOLOGY

➤ *Introduction*

This chapter outlined the research methodology that guided the study on the relationship between university students' social media behavior and their exposure to cybersecurity threats. It described the research design, study area, study population, sampling strategies, data collection methods, measurement of variables, validity and reliability considerations, data analysis approaches, ethical protocols, and anticipated limitations. The chosen methodology ensured empirical rigor, contextual appropriateness, and alignment with the study's mixed-methods philosophy.

➤ *Research Design*

The study adopted a cross-sectional, sequential mixed-methods design, beginning with a quantitative phase followed by a qualitative explanatory phase. This design allowed for the identification of patterns in student social media behavior and associated cybersecurity threats using structured questionnaires. The subsequent qualitative phase involved in-depth interviews to contextualize and explain the quantitative findings. This approach aligned with [16] recommendation for exploring emerging behavioral phenomena, especially where local literature was limited. The cross-sectional design enabled data collection at a single point in time, which was appropriate for a one-month study duration.

➤ *Study Area and Population*

The study was conducted in three higher learning institutions in Uganda:

- Victoria University (Kampala): An urban private university
- Ndejje University: An institution with campuses in both central and rural areas
- YMCA Vocational Institute (Kampala): A vocational and technical training institution

The target population consisted of undergraduate students aged 18–30, as this demographic represented the most active users of social media and the most digitally exposed age bracket [9]. A projected population of approximately 12,000 students across the three institutions formed the sampling frame.

➤ *Sample Size and Sampling Techniques*

Based on [17], a population of 12,000 yielded a minimum representative sample size of 373 students. The sample was proportionally allocated across the three institutions. Stratified random sampling was first used to segment students by institution and academic year. Simple random sampling was then employed within each stratum to select participants for the quantitative phase. However, due to logistical constraints and the one-month data collection timeframe, 158 valid questionnaires were fully completed and returned, representing a response rate of 79%. This response rate was considered adequate for statistical analysis and generalizability within the study's scope [18].

For the qualitative phase, purposive sampling was used to select key informants, such as ICT administrators, student leaders, and cybersecurity instructors, who could offer deeper insight into institutional practices and behavioral dynamics. A total of 6–8 interviews were conducted in this phase.

➤ *Data Sources*

The study relied on primary data, collected directly from students and key informants. The mixed-methods design enhanced data triangulation and interpretation by combining empirical breadth with contextual depth.

➤ *Data Collection Instruments*

• *Structured Questionnaire (Quantitative Phase):*

This consisted of closed-ended and Likert-scale items, divided into five sections based on the study objectives: platform use, risky behaviors, types of threats, awareness, and behavioral correlation. The instrument was self-administered in both hardcopy and Google Forms formats, depending on institutional context and logistical feasibility.

• *Interview Guide (Qualitative Phase):*

A semi-structured guide was used during one-on-one interviews with key informants. The guide included open-ended questions exploring trends in student behavior,

awareness campaigns, institutional responses, and experiences with cyber incidents.

➤ *Measurement of Variables*

• *Social Media Behavior (Independent Variable):*

This was measured across five indicators: frequency of platform use, oversharing tendencies, password reuse, clicking unverified links, and failure to activate privacy settings. Items were rated on a 5-point Likert scale (from "Never" to "Always").

• *Cybersecurity Threat Exposure (Dependent Variable):*

This was measured by student-reported experiences of phishing, identity theft, impersonation, and account compromise. Data were collected on frequency (count) and severity (Likert scale of impact).

• *Cybersecurity Awareness (Moderating Variable):*

This was measured through multiple-choice knowledge tests (e.g., identifying phishing messages) and perception items (e.g., self-efficacy and perceived vulnerability).

• *Qualitative Variables:*

These focused on themes such as digital norms, institutional cybersecurity culture, student motivation for risky behavior, and responses to threat experiences.

➤ *Validity and Reliability*

• *Validity:*

Validity was ensured through expert review of instruments. Three cybersecurity scholars and two behavioral researchers assessed the questionnaire and interview guide for content relevance, clarity, and representativeness. The Content Validity Index (CVI) was calculated to validate the instrument.

• *Reliability:*

Reliability was measured using Cronbach's Alpha for the Likert-scale sections of the questionnaire. An alpha value of ≥ 0.70 was accepted as the threshold for internal consistency [18]. A pilot test involving 30 students (excluded from the main study) was conducted to refine the instruments.

➤ *Ethical Considerations*

The following ethical protocols were observed:

- **Voluntary Participation:** All respondents were informed of their rights, and consent forms were signed.
- **Confidentiality:** Personal identifiers were anonymized. Data were stored on encrypted devices and cloud folders with restricted access.
- **Permission:** Letters from each participating university were obtained before data collection began.
- **Integrity:** Data were collected and reported honestly, without manipulation or falsification of results.

➤ Data Analysis

- *Quantitative Data Analysis:*

Quantitative data were analyzed using SPSS version 26. Descriptive statistics (frequencies, means, percentages) were used to summarize usage patterns and threat prevalence. Inferential statistics, including Pearson correlation and chi-square tests, were used to test relationships between behaviors and threat exposure.

- *Qualitative Data Analysis:*

Qualitative data underwent thematic analysis using NVivo software. Interview transcripts were analyzed for emergent themes related to risk perception, institutional culture, digital norms, and awareness gaps. Patterns were categorized and then compared to quantitative findings in a triangulation matrix to strengthen interpretation and explanatory power.

➤ Anticipated Limitations and Delimitations

- *Time Constraint:*

Given the one-month period, data collection was tightly scheduled. To mitigate this, online tools and trained assistants were used to increase speed and efficiency.

- *Self-Report Bias:*

As the study relied on self-reported behaviors, some students may have underreported risky practices. To reduce this, anonymity and confidentiality were emphasized.

- *Access Restrictions:*

Some universities delayed granting research clearance. Early engagement with institutional authorities was prioritized to address this challenge.

- *Gender Distribution of Respondents:*

- *Technological Gaps:*

Students with limited digital access may have been underrepresented. Hybrid data collection (digital and paper) helped mitigate exclusion.

IV. ANALYSIS

➤ Introduction

This chapter presents the analysis, presentation, and interpretation of data collected from 158 respondents across four higher learning institutions in Uganda: Victoria University, Cavendish University, Ndejje University, and YMCA Vocational Institute. The findings are organized according to the study objectives, which sought to: identify the most commonly used social media platforms by students; assess the prevalence of risky social media behaviors; determine the types and frequency of cybersecurity threats experienced; evaluate students' awareness and understanding of cybersecurity risks; and examine the correlation between specific social media behaviors and reported cyber incidents. Data were analyzed using descriptive and inferential statistics, with results presented in tables and figures accompanied by interpretive narratives.

➤ Response Rate and Demographic Characteristics of Respondents

- *Response Rate:*

The study targeted 200 students across the four institutions based on [17] sample size determination table. However, due to logistical constraints and the one-month data collection timeframe, 158 valid questionnaires were fully completed and returned, representing a response rate of 79%. This response rate is considered adequate for statistical analysis and generalizability within the study's scope [18].

Table 1 Gender Distribution of Respondents

Gender	Frequency	Percent
Female	46	29.1
Male	112	70.9
Total	158	100.0

The results in Table 1 reveal a significant gender disparity in the sample, with male respondents (70.9%) outnumbering female respondents (29.1%) by more than two to one. This distribution may reflect the enrolment patterns in the participating institutions, particularly at Victoria University which contributed the majority of respondents (73.4%). The higher proportion of male respondents could also be attributed to greater willingness

among male students to participate in surveys on digital behavior and cybersecurity topics. While the gender imbalance is notable, the sample size of 46 female respondents remains sufficient for comparative analysis and does not compromise the validity of the overall findings. Similar studies in the East African context have reported comparable gender distributions in technology-focused research [7].

- *Distribution of Respondents by University/Institution:*

Table 2 Distribution of Respondents by Institution

Institution	Frequency	Percent
Cavendish University	25	15.8
Ndejje University	14	8.9
Victoria University	116	73.4
YMCA Vocational Institute	3	1.9
Total	158	100.0

Table 2 indicates that Victoria University contributed the largest proportion of respondents (73.4%, n=116), followed by Cavendish University (15.8%, n=25), Ndejje University (8.9%, n=14), and YMCA Vocational Institute (1.9%, n=3). This distribution reflects the accessibility and institutional cooperation levels during the data collection period. Victoria University's dominance in the sample is justifiable given its urban

location and the researchers' institutional connections, which facilitated higher response rates. The inclusion of multiple institution types—private urban (Victoria and Cavendish), public with rural-urban presence (Ndejje), and vocational (YMCA)—provides diversity in the sample despite the unequal distribution. This diversity enhances the study's ability to capture varied experiences across different higher education contexts in Uganda.

- *Age Distribution of Respondents:*

Table 3 Age Distribution of Respondents

Age Bracket	Frequency	Percent
18-20	18	11.4
21-23	63	39.9
24-26	33	20.9
27-30	22	13.9
31-35	22	13.9
Total	158	100.0

The age distribution in Table 3 shows that the majority of respondents (51.3%) fall within the 21-23 age bracket, which is consistent with the typical undergraduate student population in Uganda. Combined with the 18-20 bracket (11.4%), students aged 23 and below constitute 62.7% of the sample. This aligns with the study's target population of young adults aged 18-30, who represent the most active users of social media and the most digitally

exposed demographic [9]. The presence of older students (27-35 years) at 27.8% reflects the growing trend of mature-age enrolment in Ugandan universities, particularly in private institutions and vocational programs. This age diversity enriches the study by capturing cybersecurity experiences across different maturity levels and digital exposure histories.

- *Gender by Institution Cross-Tabulation:*

Table 4 Gender * Institution Cross-Tabulation

Gender	Cavendish University	Ndejje University	Victoria University	YMCA	Total
Female	11	4	30	1	46
Male	14	10	86	2	112
Total	25	14	116	3	158

Table 4 reveals that the gender distribution pattern is consistent across institutions, with males outnumbering females in all four settings. Victoria University shows the most pronounced difference (86 males vs. 30 females), which heavily influences the overall gender distribution. This cross-tabulation confirms that the gender imbalance

is not institution-specific but rather a consistent characteristic of the sample. The finding suggests that future research in this area may need to employ targeted strategies to ensure more balanced gender representation, possibly through female-focused data collection sessions or incentives.

- *Year of Study by Institution Cross-Tabulation:*

Table 5 Year of Study by Institution Cross-Tabulation

Year of Study	Cavendish University	Ndejje University	Victoria University	YMCA	Total
1st Year	18	1	87	0	106
2nd Year	0	0	14	1	15
3rd Year	7	11	14	1	33
4th Year+	0	2	1	1	4
Total	25	14	116	3	158

Table 5 shows a predominance of first-year students (67.1%, n=106) in the sample, particularly at Victoria University where 87 out of 116 respondents were in their first year. This concentration of first-year students is noteworthy as they represent the newest entrants to university life and may have different social media behaviors and cybersecurity awareness levels compared to continuing students. Third-year students constitute 20.9%

(n=33) of the sample, while second-year and fourth-year students are minimally represented. The overrepresentation of first-year students suggests that findings may reflect the behaviors and experiences of students in their initial university year, which could be characterized by heightened social media activity for social integration and less developed cybersecurity practices.

➤ *Most Commonly Used Social Media Platforms by Students*

- *Percentage Distribution of Social Media Platform Use:*

Table 6 Frequency of Social Media Platform Usage Among Students (%)

Platform	Never (%)	Rarely (%)	Sometimes (%)	Often (%)	Very Frequently (%)	Total (%)
WhatsApp	0.0	0.6	2.5	24.1	72.8	100
Facebook	23.4	40.5	19.0	8.9	8.2	100
Instagram	20.9	21.5	25.3	21.5	10.8	100
TikTok	14.6	5.7	20.3	22.2	37.3	100
X (Twitter)	20.3	27.8	18.4	15.2	18.4	100
Snapchat	37.3	26.6	14.6	9.5	12.0	100
Telegram	29.7	25.3	23.4	13.3	8.2	100

✓ *WhatsApp Dominance:*

The results in Table 6 reveal WhatsApp as the undisputed leading social media platform among university students, with an astonishing 96.9% of respondents using it either "Often" (24.1%) or "Very Frequently" (72.8%). Notably, zero respondents reported never using WhatsApp, and only 0.6% (one respondent) reported rare use. This near-universal adoption confirms WhatsApp's integration into every aspect of student life—academic communication (class groups), social interaction (friendship groups), family contact, and entertainment. The platform's end-to-end encryption, multimedia sharing capabilities, and low data consumption make it particularly suited to the Ugandan context where mobile data costs remain relatively high. This finding aligns with [9] reports indicating over 90% WhatsApp penetration among Ugandan youth.

✓ *TikTok's Rising Popularity:*

TikTok emerges as the second most frequently used platform, with 37.3% of students using it "Very Frequently" and an additional 22.2% using it "Often"—together accounting for 59.5% of respondents. Only 14.6% reported never using TikTok, indicating significant penetration. This finding reflects global trends in short-form video content consumption among young adults and suggests that entertainment-driven platforms are capturing substantial student attention. The visual and creative

nature of TikTok appeals to university students seeking self-expression and social connection.

✓ *Instagram's Moderate Engagement:*

Instagram shows a more balanced distribution across all usage categories, with 21.5% using it "Often" and 10.8% "Very Frequently." However, 42.4% of respondents use it "Rarely" (21.5%) or "Never" (20.9%), indicating that while Instagram has a dedicated user base, it has not achieved the universal adoption of WhatsApp. This moderate engagement may reflect Instagram's higher data consumption and the preference for text-light, visual content among specific student segments.

✓ *Facebook's Declining Relevance:*

Facebook exhibits the highest "Rarely" usage at 40.5%, with 23.4% never using the platform. Only 17.1% use Facebook "Often" or "Very Frequently." This pattern confirms global trends of younger users migrating away from Facebook toward newer platforms like TikTok and Instagram. Facebook's association with older demographics and corporate presence may reduce its appeal among university students seeking peer-exclusive spaces.

✓ *X (Twitter) as a Niche Platform:*

Twitter shows a diverse usage pattern with relatively even distribution across categories—27.8% "Rarely,"

20.3% "Never," 18.4% "Sometimes," and 33.6% using it "Often" or "Very Frequently." This suggests Twitter serves a specific niche of students interested in news, public discourse, and professional networking rather than casual social interaction.

✓ *Snapchat and Telegram as Secondary Platforms:*

Snapchat has the highest "Never" usage at 37.3%, indicating limited adoption among Ugandan university students compared to global trends. Telegram shows similar patterns with 29.7% never using it, though its usage for academic and professional groups may grow given its superior file-sharing capabilities compared to WhatsApp.

➤ *Gender-Based Analysis of Platform Usage:*

Table 7 Gender-Based Whatsapp Usage Cross-Tabulation

Gender	Often	Rarely	Sometimes	Very Frequently	Total
Female	11	1	1	33	46
Male	27	0	3	82	112
Total	38	1	4	115	158

Table 7 demonstrates that WhatsApp usage patterns are consistent across genders, with both male (73.2% of males) and female (71.7% of females) students predominantly using the platform "Very Frequently." This

gender parity in WhatsApp adoption reinforces its position as a universal communication tool transcending gender difference.

Table 8 Gender * Tiktok Usage Cross-Tabulation

Gender	Never	Often	Rarely	Sometimes	Very Frequently	Total
Female	5	9	2	6	24	46
Male	18	26	7	26	35	112
Total	23	35	9	32	59	158

TikTok usage reveals interesting gender dynamics. While 52.2% of female students use TikTok "Very Frequently" compared to 31.3% of males, the absolute numbers show more male frequent users (35 vs. 24 females) due to the sample composition. Notably, only 10.9% of females reported never using TikTok compared

to 16.1% of males, suggesting slightly higher female engagement with the platform. This aligns with research indicating women's preference for visually-oriented social media platforms for self-expression and community building [1].

Table 9 Gender* Instagram Usage Cross-Tabulation

Gender	Never	Often	Rarely	Sometimes	Very Frequently	Total
Female	13	11	8	9	5	46
Male	20	23	26	31	12	112
Total	33	34	34	40	17	158

Instagram shows relatively balanced gender patterns, with 23.9% of females and 20.5% of males using it "Often" or "Very Frequently." However, 28.3% of females reported never using Instagram compared to 17.9% of males. This suggests Instagram appeals to a

specific subset of students regardless of gender, but male students show slightly higher engagement levels, possibly driven by interests in celebrity culture, sports content, and meme sharing.

Table 10 Gender * Facebook Usage Cross-Tabulation

Gender	Never	Often	Rarely	Sometimes	Very Frequently	Total
Female	14	4	13	12	3	46
Male	23	10	51	18	10	112
Total	37	14	64	30	13	158

Facebook usage patterns reveal that 30.4% of females and 20.5% of males never use the platform, while 45.5% of males use it "Rarely" compared to 28.3% of females. This indicates that among the declining Facebook user base, male students maintain slightly higher

engagement levels, possibly for academic group participation and access to information from institutional pages that continue to use Facebook as a broadcast medium.

Table 11 Gender * 10 (Twitter) Usage Cross-Tabulation

Gender	Never	Often	Rarely	Sometimes	Very Frequently	Total
Female	13	4	15	7	7	46
Male	19	20	29	22	22	112
Total	32	24	44	29	29	158

Twitter usage shows 32.6% of females and 37.5% of males using it "Often" or "Very Frequently," indicating Twitter as a platform with relatively higher male engagement. The platform's text-heavy nature and focus

on news, politics, and professional discourse may appeal more to male students, though the difference is not dramatic.

Table 12 Gender * Snapchat Usage Cross-Tabulation

Gender	Never	Often	Rarely	Sometimes	Very Frequently	Total
Female	6	8	11	11	10	46
Male	53	7	31	12	9	112
Total	59	15	42	23	19	158

Snapchat reveals the most striking gender disparity. While only 13.0% of females never use Snapchat, a staggering 47.3% of males report never using it. Female students show much higher engagement, with 21.7% using it "Very Frequently" compared to 8.0% of males.

This suggests Snapchat has become a predominantly female-oriented platform in the Ugandan university context, possibly due to its focus on visual cication, filters, and ephemeral content that appeals more to female social interaction patterns.

Table 13 Gender * Telegram Usage Cross-Tabulation

Gender	Never	Often	Rarely	Sometimes	Very Frequently	Total
Female	19	6	10	9	2	46
Male	28	15	30	28	11	112
Total	47	21	40	37	13	158

Telegram usage shows 41.3% of females and 25.0% of males never using the platform, while 23.2% of males use it "Often" or "Very Frequently" compared to 17.4% of females. This indicates Telegram as a platform with

moderate male bias, possibly driven by its popularity among tech-savvy students and those in professional or academic circles requiring advanced file-sharing capabilities.

➤ Prevalence of Risky Social Media Behaviors Among Students

Table 14 Prevalence of Risky Social Media Behaviors (%)

Risky Behavior	Never (%)	Rarely (%)	Sometimes (%)	Often (%)	Always (%)
I post personal photos publicly	20.9	38.6	23.4	7.6	9.5
I accept friend requests from people I don't know	22.8	29.1	28.5	11.4	8.2
I reuse passwords across multiple accounts	22.8	19.0	24.7	15.8	17.7
I click links without checking the source	49.4	31.0	12.7	4.4	2.5
I use my real name & date of birth publicly	15.2	17.7	28.5	13.9	24.7
I rarely update my passwords	12.0	34.2	22.8	13.3	17.7

The findings reveal concerning patterns of personal information sharing. Real name and date of birth exposure emerges as the most prevalent risky behavior, with 67.1% of students engaging in this practice at varying frequencies—24.7% "Always" publicly display this information, 13.9% "Often," and 28.5% "Sometimes." Only 15.2% reported never sharing this sensitive information. This behavior is particularly dangerous as name and date of birth combinations are commonly used for identity verification, making students vulnerable to identity theft and account takeover attacks. Cybercriminals can use this publicly available information

to answer security questions, impersonate students, or conduct targeted social engineering attacks [8].

Personal photo sharing shows moderate risk levels, with 38.6% "Rarely" posting photos publicly and 23.4% doing so "Sometimes." However, 17.1% post photos "Often" or "Always," exposing themselves to risks including facial recognition exploitation, photo-based impersonation, and stalking. The 20.9% who never post photos publicly demonstrate awareness of privacy risks associated with visual content.

Password reuse represents a critical security vulnerability, with 58.2% of students engaging in this practice. Specifically, 17.7% "Always" reuse passwords across multiple accounts, 15.8% "Often," and 24.7% "Sometimes." Only 22.8% reported never reusing passwords. This behavior creates cascading security risks—if one account is compromised, all accounts sharing that password become vulnerable. The prevalence of password reuse suggests students prioritize convenience over security, a finding consistent with global studies [2]. Infrequent password updates compound the password reuse problem. Only 12.0% of students "Never" exhibit this risky behavior (meaning they regularly update passwords), while 53.8% "Rarely" (34.2%) or "Sometimes" (22.8%) update passwords. More concerning, 31.0% "Often" (13.3%) or "Always" (17.7%) rarely update passwords. This indicates that most students maintain static passwords for extended periods, increasing the window of opportunity for attackers to exploit compromised credentials.

Accepting friend requests from unknown persons shows that 47.9% of students engage in this behavior "Sometimes" (28.5%), "Often" (11.4%), or "Always" (8.2%). While 22.8% "Never" accept unknown requests, the substantial minority who do so expose themselves to impersonators, scammers, and malicious actors who use fake profiles to conduct social engineering attacks. This behavior is particularly risky on platforms where private information is visible to connections.

Clicking links without checking the source shows the most positive security behavior among all risky practices. Nearly half (49.4%) of students "Never" click unverified links, and an additional 31.0% "Rarely" do so. Only 6.9% click unverified links "Often" or "Always." This pattern suggests students have internalized basic cybersecurity messaging about avoiding suspicious links, likely due to widespread public awareness campaigns about phishing and malware. However, the 19.6% who click unverified links "Sometimes" or more frequently still represent a vulnerable population requiring targeted intervention.

➤ *Types and Frequency of Cybersecurity Threats Experienced by Students*

Table 15 Prevalence of Cybersecurity Threats Among Students

Cybersecurity Threat	No (%)	Yes (%)
Account hacking	78.5	21.5
Phishing attempts	64.6	35.4
Identity theft / impersonation	79.1	20.9
Device malware via social media	84.8	15.2
Unauthorized password change	84.2	15.8

Study findings revealed that phishing emerges as the most commonly experienced cybersecurity threat, affecting 35.4% of respondents. This finding aligns with global patterns where social engineering attacks targeting human psychology remain the primary entry point for cybercriminals [1]. Phishing attempts typically arrive through direct messages on social media platforms, particularly WhatsApp and Instagram, or via emails that appear to originate from legitimate sources. The high prevalence suggests that students are regularly targeted with deceptive messages designed to steal credentials, install malware, or extract personal information.

The 64.6% who reported no phishing experiences may either have avoided such attacks or, more concerning, may have encountered phishing attempts without recognizing them—a possibility supported by the awareness findings discussed later. Given that phishing attacks are becoming increasingly sophisticated, often mimicking legitimate communications perfectly, the actual exposure rate may be higher than reported.

Account hacking affects 21.5% of students, meaning approximately one in five respondents has experienced unauthorized access to their social media accounts. This represents a significant security breach with cascading consequences, including loss of personal data, impersonation, reputational damage, and potential financial losses if accounts are used to scam the victim's

contacts. The 21.5% rate is concerning but consistent with regional studies in East Africa [12].

The mechanisms of account hacking likely include password guessing, credential theft through phishing, exploitation of password reuse across platforms, and social engineering of customer support channels. The prevalence of password reuse (58.2%) documented earlier provides a plausible explanation for the account hacking rate.

Identity theft or impersonation affects 20.9% of students, nearly identical to account hacking rates. This threat often follows account hacking—attackers use compromised accounts to impersonate victims—but can also involve creation of fake profiles using victims' photos and information. The prevalence of public personal information sharing (67.1% share real names and birth dates; 58.2% share photos publicly) provides attackers with raw materials for convincing impersonation.

Impersonation attacks have serious consequences, including reputational damage when fake accounts post inappropriate content, social harm when contacts are defrauded, and psychological distress for victims who feel violated and powerless to remove fake profiles.

Unauthorized password changes affect 15.8% of students, often representing the culmination of successful account compromise where attackers change credentials

to lock out legitimate owners. Device malware infections via social media affect 15.2% of students, typically resulting from clicking malicious links or downloading infected files shared through social platforms.

The lower prevalence of these threats compared to phishing and hacking may reflect their status as secondary

outcomes—malware often follows link-clicking, and unauthorized password changes follow account compromise. However, the 15% rates remain significant, indicating substantial numbers of students experiencing severe security incidents.

➤ *Students' Awareness and Understanding of Cybersecurity Risks on Social Platforms*

Table 16 Students' Cybersecurity Awareness and Protective Practices (%)

Awareness Statement	Strongly Disagree (%)	Disagree (%)	Sometimes (%)	Agree (%)	Strongly Agree (%)
I understand what phishing is	8.9	8.2	19.6	31.6	31.6
I can recognize a suspicious link	8.2	6.3	32.9	29.7	22.8
I use two-factor authentication (2FA)	4.4	8.9	32.3	20.9	33.5
I've received cybersecurity awareness training	16.5	20.9	20.9	24.1	17.7
I feel confident protecting my accounts	2.5	3.2	13.9	22.2	57.6

The findings reveal a critical disconnect between perceived and actual understanding of phishing. While 63.2% of students agree or strongly agree that they understand what phishing is, the threat prevalence data shows that 35.4% have experienced phishing attempts—and these likely underestimates actual exposure. More concerning, 19.6% are uncertain about their understanding ("Sometimes"), and 17.1% openly disagree that they understand phishing.

This pattern suggests that while a majority believe they understand phishing, the high success rate of phishing attempts (evidenced by account hacking and credential theft rates) indicates that this self-assessed understanding may not translate into practical detection ability. Students may know the term "phishing" without understanding its varied manifestations or possessing skills to identify sophisticated attacks. This finding aligns with [1], who found that only 23% of students could correctly identify phishing attempts despite higher self-reported awareness.

Similar patterns emerge for link recognition. While 52.5% agree or strongly agree they can recognize suspicious links, 32.9% are uncertain, and 14.5% disagree. The uncertainty rate (nearly one-third) is particularly concerning given that link-clicking represents a primary vector for malware and phishing. The finding that 19.6% of students click unverified links at least sometimes suggests that link recognition skills are not adequately developed across the student population.

The gap between confidence and actual competence in link recognition represents a dangerous vulnerability—students who overestimate their abilities may take risks they are ill-equipped to handle, exposing themselves to sophisticated attacks designed to bypass casual inspection.

Two-factor authentication (2FA) adoption shows relatively positive patterns, with 54.4% agreeing or strongly agreeing they use 2FA. However, 32.3% are inconsistent users ("Sometimes"), and 13.3% do not use 2FA at all. Given that 2FA is one of the most effective

protections against account compromise, the fact that nearly half of students do not consistently use it represents a significant security gap.

The high 2FA adoption among consistent users may reflect platform defaults (many platforms now encourage or require 2FA) rather than proactive security behavior. The substantial "Sometimes" category suggests students enable 2FA on some accounts but not others, leaving critical accounts (email, primary social media) potentially unprotected.

The most alarming finding in this section is the training gap. Only 41.8% of students agree or strongly agree they have received cybersecurity awareness training, while 37.4% disagree or strongly disagree, and 20.9% are uncertain. This means that nearly 60% of students lack clear recollection or confirmation of having received formal cybersecurity education. This finding directly validates the problem statement's assertion that cybersecurity education is not systematically integrated into higher education curricula in Uganda. Despite institutional ICT policies, students are not receiving the behavioral training necessary to protect themselves online. The training gap explains many of the risky behaviors and threat exposures documented earlier—students cannot practice what they have not been taught. Strikingly, despite limited training and knowledge gaps, 79.8% of students feel confident about protecting their accounts (22.2% agree, 57.6% strongly agree). Only 5.7% lack confidence, and 13.9% are uncertain.

This confidence-confidence gap represents a dangerous overconfidence bias in cybersecurity. Students believe they are more capable than their knowledge and behaviors suggest. This overconfidence may reduce their motivation to seek training, adopt protective tools, or exercise caution online. The Dunning-Kruger effect appears operative here—those with the least competence often overestimate their abilities the most, leaving them vulnerable to attacks they believe they can handle.

➤ *To Examine the Correlation between Specific Social Media Behaviors and Reported Cyber Incidents*

This section tests the study's hypotheses by examining relationships between specific risky behaviors and corresponding cybersecurity threats. The null

hypothesis (H_0) states there is no significant relationship between students' social media behavior and their exposure to cybersecurity threats, while the alternative hypothesis (H_1) posits a significant relationship.

• *Relationship between Password Reuse and Account Hacking:*

Table 17 Password Reuse * Account Hacking Cross-Tabulation

I reuse passwords across multiple accounts	Account Hacking: No	Account Hacking: Yes	Total
Always	17	11	28
Never	30	6	36
Often	20	5	25
Rarely	25	5	30
Sometimes	32	7	39
Total	124	34	158

The cross-tabulation reveals that among students who "Always" reuse passwords, 39.3% (11 out of 28) experienced account hacking, compared to only 16.7% (6 out of 36) of those who "Never" reuse passwords. This represents a 2.35-fold increase in hacking risk for consistent password reusers. Similarly, "Often" reusers show a 20% hacking rate, "Rarely" reusers 16.7%, and "Sometimes" reusers 17.9%.

However, the practical significance is evident—the data show a clear directional relationship where frequent password reusers experience substantially higher hacking rates. This pattern aligns with established cybersecurity research and suggests that with a larger sample, this relationship would likely achieve statistical significance.

• *Relationship between Infrequent Password Updates and Unauthorized Password Changes:*

Table 18 Rare Password Updates * Unauthorized Password Change Cross-Tabulation

I rarely update my passwords	Unauthorized Password Change: No	Unauthorized Password Change: Yes	Total
Always	25	3	28
Never	15	4	19
Often	19	2	21
Rarely	44	10	54
Sometimes	30	6	36
Total	133	25	158

The cross-tabulation shows that among students who "Always" rarely update passwords, 10.7% experienced unauthorized password changes, compared to 21.1% of those who "Never" exhibit this behavior (meaning they regularly update passwords). This counterintuitive

finding—where better password hygiene appears associated with higher risk—likely reflects the small sample size and the fact that unauthorized password changes may occur through mechanisms unrelated to password age (e.g., phishing, credential theft).

• *Relationship between Clicking Unverified Links and Phishing Attempts:*

Table 19 Clicking Unverified Links * Phishing Attempts Cross-Tabulation

I click links without checking the source	Phishing Attempts: No	Phishing Attempts: Yes	Total
Always	2	2	4
Never	51	27	78
Often	4	3	7
Rarely	35	14	49
Sometimes	10	10	20
Total	102	56	158

Table 20 Chi-Square Tests for Clicking Unverified Links and Phishing Attempts

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	3.425 ^a	4	.489
Likelihood Ratio	3.359	4	.500
N of Valid Cases	158		

- ✓ 4 Cells (40.0%) Have Expected Count Less than 5. The Minimum Expected Count is 1.42.

The cross-tabulation reveals that among students who "Sometimes" click unverified links, 50.0% (10 out of 20) experienced phishing attempts, compared to 34.6% (27 out of 78) of those who "Never" click unverified links. Students who "Always" click unverified links show a 50% phishing rate, though the small cell size (n=4) limits reliability.

The Pearson Chi-Square test yields a p-value of .489, indicating no statistically significant relationship at the .05 level. The null hypothesis cannot be rejected for this

relationship. The lack of significance may reflect the overall high phishing exposure rate (35.4%) across all behavior categories—phishing is so prevalent that even cautious students are targeted, though perhaps less successfully. Additionally, the small number of students in high-risk categories ("Always" = 4, "Often" = 7) limits statistical power to detect differences. However, the directional pattern suggests that link-clicking behavior does influence phishing exposure, with "Sometimes" and "Always" clickers showing 50% exposure rates compared to 34.6% for "Never" clickers—a 44% relative increase in risk.

- Relationship between Accepting Unknown Friend Requests and Identity Theft/Impersonation:

Table 21 Accepting Unknown Requests * Identity Theft/Impersonation Cross-Tabulation

I accept friend requests from people I don't know	Identity Theft/Impersonation: No	Identity Theft/Impersonation: Yes	Total
Always	9	4	13
Never	31	5	36
Often	13	5	18
Rarely	35	11	46
Sometimes	37	8	45
Total	125	33	158

➤ Qualitative Analysis of Open-Ended Responses

This section presents a thematic analysis of responses to three open-ended questions included in the survey. These questions sought to capture students' personal experiences, protective practices, and recommendations regarding cybersecurity. The qualitative data provides depth and context to the quantitative findings, revealing the lived experiences of students, the reasoning behind their behaviors, and their perspectives on institutional and platform-level interventions. A total of 158 respondents provided varying levels of detail in their open-ended responses, with response rates including verbatim quotations to illustrate each theme.

- Protective Measures Taken by Students:

✓ Question:

"What measures do you personally take to protect your social media accounts from cybersecurity threats?"

Students described a range of protective behaviors, from fundamental security practices to more advanced technical measures. Analysis of their responses revealed ten distinct thematic categories, with many respondents reporting multiple concurrent strategies. Table 22 presents the frequency with which each theme emerged across the sample.

Table 22 Thematic Analysis of Protective Measures Taken by Students

Theme	Frequency of Mention	Percentage of Respondents
Use of Strong Passwords	62	39.2%
Two-Factor Authentication (2FA) / Multi-Factor Authentication (MFA)	41	25.9%
Avoiding/Caution with Unknown Links	35	22.2%
Regular Password Changes	24	15.2%
Not Sharing Personal Information/Privacy Settings	18	11.4%
Not Accepting Unknown Friend Requests	12	7.6%
Using Password Managers/Biometrics	8	5.1%
Logging Out of Accounts/Not Saving Passwords	7	4.4%
Using VPN/Antivirus Software	5	3.2%
Reporting/Blocking Suspicious Accounts	4	2.5%

Note: Percentages exceed 100% as many respondents mentioned multiple measures.

✓ Use of Strong Passwords

The most frequently mentioned protective measure was the use of strong passwords, cited by 62 respondents, representing 39.2% of the sample. Students demonstrated

awareness that password strength constitutes a fundamental security control, with many describing specific strategies for creating robust passwords that would resist guessing and brute-force attacks.

A respondent from Victoria University emphasized the importance of password complexity in straightforward terms: *"I use strong passwords with combination of digits, symbols, letters both capital and small"* (Respondent 31, Male, Ndejje University). This response illustrates basic understanding of the components that contribute to password strength—character diversity and complexity.

Another student described a more comprehensive approach to password management that extends beyond mere creation: *"Strong, unique passwords for each account. Two-factor authentication (2FA) enabled everywhere. Regular review of connected apps and active sessions"* (Respondent 49, Male, Victoria University). This response reveals a sophisticated understanding that password security requires ongoing maintenance and complementary controls, including the regular auditing of third-party applications that may have access to accounts.

A third respondent highlighted the relationship between passwords and other security measures while also revealing awareness of social engineering threats: *"Setting strong password keys with numbers, letters and symbols. Someone tried to send a link from untrusted sources impersonating as a friend"* (Respondent 108, Male, Victoria University). The inclusion of the key emoji suggests the symbolic importance students attach to passwords as literal keys to their digital identities.

The emphasis on password strength indicates that basic cybersecurity messaging has successfully reached students at some level. However, as noted in the quantitative findings, the prevalence of password reuse (58.2% of students) suggests a significant disconnect between knowing about strong passwords and consistently implementing them across all accounts. This gap between knowledge and behavior represents a critical intervention point for educational programs.

✓ *Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA)*

Forty-one respondents (25.9%) explicitly mentioned using two-factor or multi-factor authentication, making this the second most cited protective measure. Students demonstrated clear understanding of 2FA's value as an additional security layer that protects accounts even when passwords are compromised.

A postgraduate student in cybersecurity provided a particularly comprehensive account of their authentication practices: *"I use 2 factor authentication for all my social media accounts. I use two multi factor authentication for login"* (Respondent 26, Male, Victoria University). This response suggests not only awareness but consistent implementation across the student's digital presence.

Another respondent described their layered security approach with notable emphasis: *"2 FACTOR AUTHENTICATION, USING STRONG PASSWORDS, REPORTING SPAM MESSAGES, BLOCKING ANY SUSPICIOUS UNKNOWN MESSAGE"* (Respondent 46, Male, Victoria University). The use of capital letters

conveys the importance this student attaches to 2FA as a cornerstone of their personal security framework.

A student from Cavendish University emphasized the universal application of this measure: *"Using two-factor authentication is the way to go. I use MFA and change of passwords"* (Respondent 141, Male, Cavendish University). The phrase "the way to go" suggests endorsement based on positive personal experience with this security control.

The relatively high mention of 2FA is encouraging and aligns with the quantitative finding that 54.4% of students use 2FA consistently. However, the notable gap between mention (25.9%) and reported usage (54.4%) suggests an interesting phenomenon: while many students use 2FA, not all think to mention it as a primary protective measure. This may indicate that for some students, 2FA has become such an integrated, default feature of platform security that it no longer registers as a conscious "measure they take"—rather, it is simply how logging in works. This interpretation, if accurate, actually represents a positive outcome of platform design that normalizes security features.

✓ *Avoiding and Exercising Caution with Unknown Links*

Thirty-five respondents (22.2%) mentioned exercising caution with links as a key protective measure. This theme reflects students' awareness that links serve as primary vectors for phishing attacks and malware distribution in the social media environment.

A respondent described their cautious approach with deliberate redundancy that emphasizes the strength of their conviction: *"Avoid unknwn links. No linking in unknown links. I don't click in links that I don't know the source"* (Respondent 9, Male, Victoria University). The repetition across three short sentences underscores the absolute nature of this student's rule—unknown links are simply not engaged with under any circumstances.

Another student expressed an even more stringent approach: *"Avoiding at all times clicking on links from unknown sources. I don't open any link sent to me"* (Respondent 100, Female, Victoria University). The phrase "at all times" indicates a consistent, unwavering policy, while the second sentence suggests this student may have adopted a zero-tolerance approach following negative experiences or effective.

A particularly insightful response revealed how students develop practical heuristics for threat detection based on psychological manipulation attempts: *"Ever received a links that if you click on it, you receive data but I just ignore them coz I feel like there's no company can just give free data"* (Respondent 67, Female, Victoria University). This quotation reveals an important informal protection mechanism—skepticism of offers that appear "too good to be true." The student has internalized a critical principle of security awareness: legitimate entities do not typically offer valuable resources through unsolicited links. This homespun heuristic serves as an

effective defense against many phishing attempts that rely on greed or urgency as psychological triggers.

✓ *Regular Password Changes*

Twenty-four respondents (15.2%) mentioned changing passwords regularly as a protective measure. This practice reflects an understanding that credentials can be compromised over time without the user's knowledge, making periodic refreshing a prudent security habit.

A respondent from Victoria University linked password changes with another protective behavior: *"Through changing passwords every month when possible and also not clicking on suspicious links being sent"* (Respondent 14, Male, Victoria University). The phrase "when possible" acknowledges practical constraints that may prevent ideal security practices, demonstrating realistic self-awareness about implementation challenges.

Another student described their routine with emphasis: *"I change passwords often. BY KEEP CHANGING PASSWORDS"* (Respondent 78, Male, Victoria University; Respondent 155, Male, Victoria University). The repetition and capitalization suggest this student considers password rotation a security priority worthy of emphasis.

A female respondent connected password practices with other protective behaviors: *"Update passwords always. Update my passwords and avoiding clicking in links and responding to suspicious messages"* (Respondent 40, Female, Ndejje University; Respondent 37, Female, Ndejje University). This response reflects a multi-faceted approach where regular password updates complement other defensive practices.

However, the quantitative finding that 31.0% of students "often" or "always" rarely update their passwords suggests a binary distribution in password hygiene behaviors. The student population appears divided between those who maintain regular update routines and those who seldom or never change passwords, with relatively few adopting intermediate positions. This polarization may reflect differing mental models of threat persistence—some students view credential compromise as a continuous risk requiring ongoing countermeasures, while others treat password setting as a one-time event.

✓ *Not Sharing Personal Information and Privacy Settings*

Eighteen respondents (11.4%) mentioned limiting personal information sharing or adjusting privacy settings as protective measures. This theme reflects awareness that oversharing creates reconnaissance opportunities for attackers and may directly expose sensitive information.

A respondent from Victoria University explained their privacy-conscious approach: *"I don't post much about myself. I rarely share my picture, I don't accept requests, I use strong passwords"* (Respondent 23, Male, Victoria University; Respondent 116, Female, Victoria University). The cumulative effect of these behaviors—

reduced posting, limited photo sharing, restricted connections, and strong authentication—creates a smaller attack surface for potential adversaries.

Another student emphasized privacy boundaries with notable clarity: *"Strongly not sharing my privacy with anyone. Not sharing login credentials. Updating password frequently"* (Respondent 96, Male, Victoria University; Respondent 156, Male, Victoria University). The phrase "strongly not sharing" conveys an intensity of commitment to privacy that goes beyond passive preference to active principle.

A female respondent from Cavendish University connected privacy practices to broader security in a comprehensive statement: *"To protect social media accounts, use strong, unique passwords, enable two-factor authentication—limit personal information shared online"* (Respondent 128, Female, Cavendish University). The structure of this response—presenting multiple controls in sequence—suggests an integrated mental model where privacy complements authentication as part of a unified security strategy.

Despite these encouraging responses, the quantitative finding that 67.1% of students publicly share their real names and birth dates presents a striking contrast. This apparent contradiction indicates that privacy awareness, while present in some students, has not translated into widespread protective behavior across the sample. The gap may reflect differences in risk perception, platform literacy, or the social pressures that incentivize information sharing despite recognized risks.

✓ *Not Accepting Unknown Friend Requests*

Twelve respondents (7.6%) specifically mentioned rejecting or avoiding friend requests from unknown persons. This behavior directly addresses the risk of social engineering through fake profiles, which may be used for reconnaissance, phishing, or credibility-building for subsequent attacks.

A respondent from Ndejje University described their response to an unwanted connection attempt: *"Not opening or accepting any friendly requests I don't know about. Blocked the request and deleted it as well"* (Respondent 34, Male, Ndejje University). The response describes a two-step process—non-acceptance followed by active removal—that eliminates any future interaction possibility with the requester.

Another student from Cavendish University described their comprehensive approach to connection management: *"I post less and don't accept random friends or even those that inbox me from no where that they want to be my friends online"* (Respondent 139, Female, Cavendish University). The phrase "from no where" captures the unexpected and context-free nature of many suspicious connection attempts, which lack any preceding interaction or mutual connection to explain the request.

A Victoria University student linked this practice to their overall security strategy: *"I don't share my password with anyone, I don't click on links I don't understand, reject friendly requests from unknown people"* (Respondent 158, Female, Victoria University). This integrated approach treats connection management as one component of a broader defensive posture rather than an isolated practice.

The relatively low mention of this protective measure (7.6%) compared to the prevalence of the risky behavior (47.9% accept unknown requests at least sometimes) suggests that many students do not recognize connection requests as a significant threat vector. The social norms of platform use—where accumulating connections is often encouraged and viewed positively—may conflict with security considerations, leaving students vulnerable to social engineering through fake profiles.

✓ *Use of Password Managers and Biometrics*

Eight respondents (5.1%) mentioned using password managers or biometric authentication (fingerprint, face ID). These represent more advanced security practices beyond basic password management, offering both stronger security and improved usability.

A respondent from Victoria University described their sophisticated, platform-integrated approach: *"Using Google's auto generated passwords. Normalizing to use Apple- Face-ID identification, Activating to Strong passwords, (2Factor Authentication)-multi-factor authentication (MFA) setup"* (Respondent 151, Male, Victoria University; Respondent 146, Male, Cavendish University). This response reveals adoption of built-in security features across multiple platforms—Google's password generation, Apple's biometric authentication, and universal 2FA—suggesting a student who has embraced the security ecosystem available through modern devices and services.

Another student mentioned biometrics as part of their authentication toolkit: *"Passwords like finger prints. Passkeys, biometrics, 2 factor authentication"* (Respondent 124, Female, Cavendish University; Respondent 137, Male, Cavendish University). The reference to "passkeys" alongside biometrics suggests awareness of emerging authentication standards that move beyond traditional passwords.

The low mention of these tools suggests that password managers and biometric authentication are not yet mainstream among Ugandan university students. Several factors may explain this limited adoption: limited awareness of these tools' existence and benefits, perceptions of complexity, concerns about biometric data privacy, or the predominance of shared devices where biometrics cannot be consistently used. This represents an opportunity for education and promotion, as these tools can simultaneously improve security and reduce user burden.

✓ *Logging Out and Not Saving Passwords*

Seven respondents (4.4%) mentioned logging out of accounts and avoiding saved passwords on shared devices. This practice is particularly important for students using university computer labs, library terminals, or friends' devices—shared computing environments where password persistence could lead to unauthorized access.

A respondent explained their approach to public device usage: *"Avoid login in to my accounts on public devices. Always logging away from others devices"* (Respondent 45, Male, Victoria University; Respondent 75, Male, Victoria University). The phrase "always logging away" suggests a consistent practice of session termination that has become habitual.

Another student described their approach to credential storage: *"I don't save passwords to my Google account such that I log out after using the account"* (Respondent 91, Male, Victoria University). This response reveals awareness that browser-based password saving, while convenient, creates risks when devices are shared or could be accessed by others.

This theme reflects awareness of the risks posed by shared computing environments common in university settings. Students who practice safe session management demonstrate understanding that security boundaries extend beyond account access to include the physical context of device usage—a sophisticated appreciation for the full attack surface.

✓ *Use of VPN and Antivirus Software*

Five respondents (3.2%) mentioned using technical protections such as VPNs or antivirus software. This low mention suggests that such tools are not widely adopted among students, possibly due to cost barriers, limited awareness, perceptions of complexity, or uncertainty about which tools are trustworthy.

A respondent mentioned these tools in combination: *"Passwords and vpn. Install anti virus utility. Through installing antivirus utility"* (Respondent 8, Male, Victoria University; Respondent 77, Female, Victoria University; Respondent 95, Female, Victoria University). The repetition of "antivirus utility" suggests this student considers endpoint protection a core security measure alongside network-level protection through VPN.

Another student described their response to a specific threat: *"I deleted the app and scanned my device with anti Spyware software"* (Respondent 30, Male, Victoria University). This response indicates not just possession of security software but its active use in response to suspected compromise—a more advanced security practice.

The limited mention of these technical controls may reflect the mobile-first nature of many students' internet access. On mobile platforms, traditional antivirus software is less common, and VPN usage, while growing, remains far from universal. Educational interventions may need to

address platform-appropriate technical protections rather than assuming desktop-oriented security models.

✓ *Reporting and Blocking Suspicious Accounts*

Four respondents (2.5%) mentioned reporting suspicious accounts or blocking threats as a protective measure. This represents active engagement with platform safety features that not only protects the individual but contributes to community safety by removing threat actors from the platform.

A respondent from Victoria University described their reporting practices: *"Reporting/blocking suspicious accounts. I report or remove accounts. i just reported their account"* (Respondent 44, Male, Ndejje University; Respondent 115, Male, Victoria University). The progression from general description to specific past action suggests this student has actually used reporting features, not just knows about them.

Another student explained their comprehensive response to a threat: *"Reported deleted and blocked the source from which it's coming from"* (Respondent 100, Female, Victoria University). This multi-step response—reporting to the platform, deleting associated content, and blocking the source—demonstrates thorough threat neutralization.

The low mention of reporting as a protective measure may reflect limited awareness of platform reporting features, skepticism about their effectiveness, or the perception that reporting is a post-incident response rather than a preventive measure. Given that reporting can remove threat actors before they harm other users, promoting this feature could have significant community-wide benefits.

✓ *No Measures Taken or Uninformed*

Six respondents (3.8%) explicitly stated that they take no protective measures or expressed complete lack of knowledge about cybersecurity. This small but concerning group represents students who are entirely vulnerable due to inaction or unawareness, constituting a high-risk population within the sample.

A respondent from Cavendish University honestly admitted their lack of engagement: *"I have no idea what this is about. I hadn't thought about it before. Nothing. No measures"* (Respondent 4, Female, Victoria University; Respondent 15, Male, Victoria University; Respondent 110, Male, Victoria University; Respondent 120, Female, Cavendish University; Respondent 136, Male, Cavendish University). This admission of complete unfamiliarity is striking in its honesty and reveals that for some students, cybersecurity has never been part of their conscious consideration—they navigate the online world without any protective framework.

Another respondent's brief response was particularly telling: *"1234567"* (Respondent 135, Female, Cavendish University). This single response—using "1234567" as a password—vividly illustrates the vulnerability of students who lack basic cybersecurity awareness. The choice of the simplest possible numeric sequence, defying every principle of password security, demonstrates either complete unawareness of risks or a decision that security is not worth the cognitive effort. Either interpretation points to urgent educational needs for this population segment.

• *Experiences with Cybersecurity Threats:*

✓ *Question:*

"Can you describe a time when you encountered a cybersecurity threat or a suspicious situation on social media? How did you handle it?"

Students reported diverse experiences with cybersecurity threats, ranging from phishing attempts to complete account takeovers. Analysis of their responses revealed six distinct threat categories, with some students reporting multiple threat types. Notably, over a quarter of respondents stated they had never encountered a threat—a finding that requires careful Table 23 presents the distribution of reported threat experiences.

Table 23 Thematic Analysis of Cybersecurity Threat Experiences

Theme	Frequency of Mention	Percentage of Respondents
Received Suspicious Links/Phishing Attempts	57	36.1%
Account Hacking/Unauthorized Access	28	17.7%
Suspicious Friend Requests/Messages from Strangers	21	13.3%
Impersonation/Fake Accounts	12	7.6%
No Experience / Never Encountered	43	27.2%
Malware/Virus Encounters	5	3.2%
Password Change Attempts	4	2.5%

✓ *Received Suspicious Links and Phishing Attempts*

The most common threat experience, mentioned by 57 respondents (36.1%), involved receiving suspicious links, typically through direct messages, WhatsApp groups, or email. These links often promised prizes, job opportunities, or free services—classic phishing lures

designed to exploit psychological triggers such as greed, curiosity, or need.

A respondent from Victoria University provided a detailed account demonstrating sophisticated threat detection: *"I got a message telling me I had won a free shopping voucher from Amazon. I had to click on the link*

to redeem the voucher. The link had a redirection and the word Amazon was misspelled i.e., Amazonn.com. I ignored the link but also reported the account to Twitter" (Respondent 26, Male, Victoria University). This response demonstrates multiple levels of security awareness: recognition of the "too good to be true" premise, careful examination of the URL for misspellings (a common phishing indicator), appropriate non-engagement with the link, and proactive reporting to the platform. The student's attention to the doubled 'n' in "Amazonn.com" shows the kind of detail-oriented skepticism that effective security education aims to cultivate.

Another student described a WhatsApp-based phishing attempt targeting group members: "Message sent in WhatsApp groups promoting job opportunities. I didn't open the link" (Respondent 45, Male, Victoria University). The simplicity of this response—recognition followed by non-action—represents the baseline of effective threat response: doing nothing in response to a suspicious prompt is often the safest course.

A particularly insightful account revealed how phishing attempts exploit psychological triggers and how awareness can interrupt the engagement cycle: "A person sent me a link which was describing a free access to an online course but instead it was requiring me to submit my essential documents and above all account details where I terminated the process immediately" (Respondent 5, Male, Victoria University). The student's decision to terminate the process when asked for sensitive information demonstrates effective threat recognition and response. The phrase "above all account details" suggests the student recognized that document requests, while potentially legitimate in some contexts, crossed a red line when combined with authentication credential demands.

Another respondent described a sophisticated impersonation-phishing combination that illustrates both the complexity of modern attacks and the protective value of secondary authentication: "I one time received a message in a WhatsApp group when my friend was hacked and I tapped into a certain UNICEF link and this guy was like send me money and I said I didn't have it coz I was suspicious. After he gave me an offer to give me that recharge money but he didn't know I had a two-step verification code in my account. After him reaching that step, he asked for it and I rejected his request and thereafter he gave up. That's when I realized it was fraud" (Respondent 103, Male, Victoria University).

This narrative is particularly valuable for understanding the student threat landscape. It reveals multiple attack layers: account compromise of a trusted contact, lures exploiting authority (UNICEF) and financial need, and active social engineering during the interaction. Crucially, the narrative illustrates how 2FA can block attackers even after a user has engaged with malicious content and interacted with the attacker. The attacker's request for the verification code represented their final obstacle, and the student's refusal—based on

suspicion but without fully understanding the threat—prevented account compromise. This is a powerful testament to the value of 2FA as a safety net when other defences fail.

✓ Account Hacking and Unauthorized Access

Twenty-eight respondents (17.7%) reported experiencing account hacking or unauthorized access to their social media accounts. These experiences ranged from minor intrusions—such as unexpected password change notifications—to complete loss of account control with significant personal and financial consequences.

A respondent described a particularly distressing experience involving a large follower account: "Actually my TikTok account of over 40k followers was hacked and taken. I reported to TikTok support but I got no reply. This made me leave TikTok for good and forever" (Respondent 85, Male, Victoria University). This account reveals the serious consequences of hacking that extend beyond mere inconvenience. The loss of 40,000 followers represents destruction of digital property and social capital built over time. The emotional impact is evident in the phrase "for good and forever," suggesting the experience was so damaging that the student permanently abandoned the platform. The reported lack of platform response to the support request compounds the initial harm with institutional neglect, potentially damaging trust in platform protections.

Another student described multiple account compromises with successful recovery: "My Instagram and LinkedIn password were changed. Managed to recover the accounts. Changed to a stronger password then 2 Authenticator added using my mobile number" (Respondent 154, Male, Victoria University). This response demonstrates that recovery is possible and that experience with compromise can lead to improved security practices—the student added 2FA following the incident, representing learning through adverse experience.

A respondent from Ndejje University reported ongoing compromise: "My Twitter account was hacked and can't access it for the moment" (Respondent 40, Female, Ndejje University). The phrase "for the moment" suggests either hope for eventual recovery or uncertainty about the account's permanent status, reflecting the limbo state that compromised account victims often experience.

A particularly concerning account described cascading consequences affecting the victim's social network: "That time my WhatsApp was hacked and I was logged out and I couldn't access my account and they started sending messages to my contacts. But all I did was to report stolen account and it was instantly blocked and given 30 days before I can access it again" (Respondent 46, Male, Victoria University).

This response reveals a critical gap in platform recovery mechanisms. The 30-day lockout period, while presumably intended to secure the account, leaves victims

unable to communicate with or warn their contacts, while attackers continue to exploit their identity during the lockout window. Contacts receiving messages from the compromised account during this period have no way to know the legitimate user is locked out, making the platform's security response potentially counterproductive for harm reduction. This represents an opportunity for platform improvement—faster verification processes or immediate notification to contacts could reduce secondary harm.

✓ *Suspicious Friend Requests and Messages from Strangers*

Twenty-one respondents (13.3%) reported receiving suspicious friend requests or messages from unknown individuals. These often served as the initial contact in social engineering attempts, with attackers using direct engagement to build rapport or extract information.

A respondent from Cavendish University described a common scam narrative with effective response: *"I recently have been receiving random texts from WhatsApp people telling that they are abroad and they have sickly people and they hope to use my help to help their relatives and I could immediately reject and block them"* (Respondent 139, Female, Cavendish University). This account describes the "relative in distress" ploy—a classic social engineering narrative that exploits empathy and urgency. The student's response of immediate rejection and blocking demonstrates effective threat recognition and decisive action.

Another student received a more directly threatening communication: *"I was threatened with death"* (Respondent 61, Male, Victoria University). This brief but chilling response indicates that cybersecurity threats can escalate to physical threats, with serious psychological impacts extending beyond the digital realm. Such experiences blur the boundary between online and offline safety and may require responses beyond technical measures, including legal or law enforcement involvement.

A female respondent described a privacy-invasive approach: *"I got a message from an unknown number asking me personal questions I immediately blocked the number"* (Respondent 94, Female, Victoria University). The recognition that personal questions from unknown sources represent a threat, and the immediate blocking response, demonstrates effective security instincts even without formal training.

✓ *Impersonation and Fake Accounts*

Twelve respondents (7.6%) reported encountering impersonation—either of themselves or people they know. This threat often accompanies account hacking or involves creation of fake profiles that mimic real individuals to deceive their contacts.

A respondent from Victoria University described their response to impersonation: *"Someone impersonating and I handled this by involving friend with IT knowledge"*

(Respondent 66, Male, Victoria University). This response highlights the value of peer support and technical knowledge within students' social networks. The student recognized that addressing impersonation required expertise beyond their own and appropriately sought help from a trusted knowledgeable source—an important strategy when facing unfamiliar threats.

Another student observed impersonation of a friend and responded in a way that protected both self and others: *"A close friend's WhatsApp was hacked and started posting malicious links, but I was luckily skeptical and suspicious of the links. So I avoided them and helped them contact the other victims of the attack"* (Respondent 153, Male, Victoria University). This account demonstrates how skepticism protects not only the individual but enables them to help others—creating a ripple effect of protection. The student's recognition that the hacked account represented a threat to mutual contacts, and their active assistance in warning others, shows prosocial security behavior that benefits the entire community.

A respondent from Cavendish University described their response to Facebook impersonation: *"In 2019-November, when someone else cracked and impersonated my fb account—I immediately changed the password and connecting my network to Virtual Private Network (VPN)"* (Respondent 146, Male, Cavendish University). This response combines immediate credential reset with network-level protection, suggesting the student may have been concerned about ongoing surveillance or further compromise attempts.

✓ *No Experience or Never Encountered*

Forty-three respondents (27.2%) stated that they had never encountered a cybersecurity threat. This finding must be interpreted cautiously—it may reflect genuine lack of exposure, but could also indicate that some threats went unrecognized, a possibility supported by other findings in this study.

Representative responses in this category included: *"None so far"* (Respondent 9, Male, Victoria University); *"I have never experienced it"* (Respondent 67, Female, Victoria University); *"Not applicable"* (Respondent 134, Female, Cavendish University); *"I haven't experienced"* (Respondent 23, Male, Victoria University); and simply *"Never"* (Respondent 27, Male, Victoria University; Respondent 137, Male, Cavendish University).

Given that 35.4% of students reported phishing attempts in the quantitative section, the 27.2% claiming no experience in the qualitative responses presents an interesting contrast. Several explanations may account for this discrepancy. First, the qualitative sample may represent a different subsection of the overall respondent pool. Second, and more concerning, some phishing attempts may have gone unrecognized as threats by these students—they may have received malicious links but not identified them as such, or may have experienced account compromises they attributed to other causes. This interpretation is supported by the awareness findings

showing that 17.1% of students do not understand phishing, suggesting a significant population lacks the threat literacy to recognize attacks when they occur.

- *Response Strategies to Threats:*
For students who reported experiencing threats, analysis revealed eight distinct response strategies,

ranging from passive ignoring to active technical countermeasures. Table 24 presents the frequency of each response strategy among those who reported threat experiences.

Table 24 Thematic Analysis of Response Strategies to Threats

Response Strategy	Frequency of Mention	Percentage of Those Who Experienced Threats
Ignored/Did Not Click/Deleted	42	36.5%
Blocked the Sender/Account	21	18.3%
Changed Password	18	15.7%
Reported to Platform	12	10.4%
Logged Out/Recovered Account	8	7.0%
Contacted Support/Sought Help	7	6.1%
Confirmed with Friend (for impersonation)	5	4.3%
Scanned Device/Used Antivirus	3	2.6%

The most common response strategy, mentioned by 42 respondents (36.5% of those who experienced threats), was simply ignoring the threat, not clicking links, or deleting the message. This passive but effective strategy reflects the "better safe than sorry" approach that security educators often recommend as a first line of defense.

Representative responses in this category captured the range of passive but effective responses: *"I ignored unknown links"* (Respondent 13, Male, Victoria University); *"I rejected the invitation to click"* (Respondent 28, Male, Victoria University); *"I put it in spam and reported it"* (Respondent 29, Male, Victoria University) — this last response combines passive (spam classification) with active (reporting) elements; *"I just ignored it"* (Respondent 50, Male, Victoria University); and *"I withheld from tapping on the link"* (Respondent 90, Female, Victoria University).

The prevalence of this response strategy is encouraging, as non-engagement with suspicious content represents a foundational security behavior that prevents many attacks from progressing. However, it also suggests that many students lack confidence in more active response strategies or view themselves as having no agency beyond avoidance.

Twenty-one respondents (18.3%) reported blocking the sender or account associated with the threat. This active response prevents further contact and potential future threats from the same source, representing a step beyond mere ignoring.

Representative responses included: *"Blocked the request and deleted it as well"* (Respondent 34, Male, Ndejje University)—this combination of blocking and deletion ensures complete removal; *"I blocked the suspicious link"* (Respondent 155, Male, Victoria University)—while one cannot strictly "block a link," this phrasing likely means blocking the sender of the link; *"I blocked my own sim and account and registered for a new one"* (Respondent 98, Female, Victoria University)—this

extreme response suggests the student considered the compromise so severe that complete account replacement was the safest option; and *"I immediately blocked the number"* (Respondent 94, Female, Victoria University)—the word "immediately" suggests decisive action without hesitation.

Blocking represents a more empowered response than ignoring, as it actively removes the threat source from the student's digital environment. Teaching students that they have this power—and that using it is appropriate, not rude—could encourage more active threat neutralization.

Eighteen respondents (15.7%) responded to threats by changing their passwords. This reactive measure addresses the possibility that credentials may have been compromised, either through the current incident or previous unknown exposures.

Representative responses included: *"Immediately changed the password"* (Respondent 7, Male, Victoria University); *"I reset my password immediately after suspicion"* (Respondent 129, Male, Cavendish University)—the phrase "after suspicion" indicates the student acted on suspicion alone, without waiting for confirmation of compromise; and *"I changed the password and added 2FA"* (Respondent 117, Male, Victoria University)—this response adds an additional security layer, representing learning and improvement following the threat experience.

Password changing as a response strategy is most effective when done promptly and when the new password is strong and unique. Students who change passwords following threats demonstrate understanding that credentials may be compromised and that proactive replacement is necessary.

Twelve respondents (10.4%) utilized platform reporting mechanisms to flag threats. This proactive response helps protect not only the individual but also the

broader community by enabling platform action against threat actors.

Representative responses included: *"I reported the account to Twitter"* (Respondent 26, Male, Victoria University); *"I reported them in the application"* (Respondent 141, Male, Cavendish University); and *"Reported the account as spam"* (Respondent 143, Female, Cavendish University).

The use of platform reporting features represents relatively sophisticated threat response, as it requires knowledge of these features' existence, confidence in their use, and willingness to invest time in community protection. Promoting reporting as a normative response to threats could increase its adoption and enhance platform-wide security. Eight respondents (7.0%) described logging out of accounts or going through account recovery processes. These responses were common among those who experienced actual account compromise requiring session termination or credential recovery.

Representative responses included: *"I logged out my account and changed the password"* (Respondent 60, Male, Victoria University)—this combination of logout and password change ensures any existing sessions are terminated; *"I signed in back since I was logged out"* (Respondent 93, Male, Victoria University)—this suggests the student was unexpectedly logged out, likely by an attacker, and had to re-authenticate; and *"Managed to recover the accounts"* (Respondent 154, Male, Victoria University)—this reflects successful navigation of platform recovery processes.

Account recovery represents a higher-stakes response strategy, as it requires interaction with platform support systems and may involve identity verification. Students who successfully recover accounts demonstrate persistence and platform literacy.

Seven respondents (6.1%) sought external help, either from platform support or knowledgeable individuals. This strategy recognizes that some threats require expertise beyond the individual's capacity and that seeking help is an appropriate response.

Representative responses included: *"I contacted support"* (Respondent 17, Male, YMCA); *"Engaged the social media app developers for assistance"* (Respondent 56, Male, Victoria University); and *"Involving friend with IT knowledge"* (Respondent 66, Male, Victoria University).

The recognition that some threats require expert intervention is an important aspect of security maturity. Students who seek help demonstrate appropriate humility about their own capabilities and awareness that support resources exist.

Five respondents (4.3%) described confirming suspicious communications with the person being

impersonated before taking action. This social verification strategy is highly effective against impersonation attacks, as it uses an out-of-band communication channel to verify identity.

A respondent provided an excellent example of this sophisticated response: *"I noticed a close friend's Twitter (X) account suddenly posting odd, spammy links. I knew it was hacked. Instead of engaging with the posts, I immediately texted her directly to confirm the breach. She wasn't aware. I advised her to start the password reset and account recovery process with Twitter (X) and to warn her friends not to click any links"* (Respondent 49, Male, Victoria University).

This response demonstrates multiple advanced security concepts: recognition of compromise indicators (sudden posting of spammy links), appropriate non-engagement with suspicious content, out-of-band verification through an alternative communication channel, and prosocial assistance to the compromised friend including specific recovery advice. The student essentially served as an incident responder for their friend, containing the attack's spread and facilitating recovery. This represents an ideal model of peer-to-peer security support within social networks.

Three respondents (2.6%) mentioned using antivirus software or scanning their devices in response to threats. This technical response is appropriate when malware infection is suspected, such as after clicking a malicious link or downloading suspicious content.

A respondent described their post-incident response: *"I deleted the app and scanned my device with anti Spyware software"* (Respondent 30, Male, Victoria University). This two-step response—removal of the suspicious application followed by security scanning—demonstrates thorough remediation practices.

The low mention of this response strategy may reflect the mobile-centric nature of many students' device usage, where traditional antivirus scanning is less common. However, as mobile threats increase, promoting endpoint security practices for all device types becomes increasingly important.

• *Recommendations for Universities and Social Media Platforms:*

✓ *Question:*

"In your opinion, what steps should universities or social media platforms take to better educate students on cybersecurity and protect them from online threats?"

Students offered numerous recommendations spanning institutional education, platform design, and community engagement. Analysis revealed eleven distinct recommendation themes, with strong emphasis on structured learning opportunities and practical training. Table 25 presents the distribution of these recommendations.

Table 25 Thematic Analysis of Student Recommendations

Recommendation Theme	Frequency of Mention	Percentage of Respondents
Cybersecurity Training/Workshops/Seminars	78	49.4%
Integrate Cybersecurity into Curriculum	32	20.3%
Awareness Campaigns/Sensitization	28	17.7%
Practical/Hands-On Training Sessions	18	11.4%
Mandatory/Compulsory Training for All Students	15	9.5%
Platform Security Features/Improvements	14	8.9%
Regular/Continuous Training Programs	12	7.6%
Real-Life Examples/Case Studies	8	5.1%
Guest Lectures/Industry Experts	6	3.8%
Use of Media (TV, Radio, Social Media Ads)	5	3.2%

✓ *Cybersecurity Training, Workshops, and Seminars*

The most frequently mentioned recommendation, cited by 78 respondents (49.4%), was the need for universities to organize cybersecurity training, workshops, or seminars. Students clearly expressed a desire for structured learning opportunities that would build their knowledge and skills in a systematic way.

A respondent from Victoria University stated the need clearly: *"More cyber security trainings. Having regular cyber security awareness programs and testing the students on their knowledge about cybersecurity"* (Respondent 17, Male, YMCA; Respondent 50, Male, Victoria University). The inclusion of "testing" suggests this student values not just exposure to information but verification that learning has occurred—assessment as a component of effective education.

Another student emphasized the importance of inclusivity in training offerings: *"Cyber security awareness training to all university students whether they do computing or not"* (Respondent 34, Male, Ndejje University). This recommendation reflects recognition that cybersecurity is not merely a technical specialty but a universal life skill needed by all students regardless of discipline. The explicit call for inclusion of non-computing students suggests that current offerings may be concentrated in technical programs, leaving others underserved.

A respondent from Cavendish University provided more specific recommendations about training content: *"Universities should organize regular cybersecurity awareness sessions and workshops to teach students how to identify scams, phishing attempts, and fake accounts"* (Respondent 143, Female, Cavendish University). The focus on identification skills—recognizing specific threat types—reflects students' desire for actionable knowledge they can apply in their daily online activities.

The overwhelming demand for training across disciplines reflects students' recognition that cybersecurity is a universal life skill, not just an IT specialization. This near-consensus (49.4%) represents a clear mandate for universities to expand cybersecurity education offerings.

✓ *Integrate Cybersecurity into Curriculum*

Thirty-two respondents (20.3%) recommended that cybersecurity be formally integrated into university curricula, either as standalone courses or as modules within existing programs. This theme reflects understanding that one-off interventions are insufficient—cybersecurity education must be systematic and sustained.

A respondent from Victoria University proposed comprehensive integration: *"Integrate cybersecurity into curricula across disciplines, offering workshops, simulations, and hands-on training"* (Respondent 128, Female, Cavendish University). This recommendation combines curriculum integration with specific pedagogical approaches (workshops, simulations, hands-on training), suggesting the student has considered not just what should be taught but how it should be taught.

Another student suggested targeted integration at key points in the student journey: *"Include cybersecurity topics in ICT or orientation programs for new students"* (Respondent 143, Female, Cavendish University). This recommendation recognizes orientation as a teachable moment when new students are forming their online behavior patterns for the university context.

A postgraduate student emphasized foundational education with a brief but powerful statement: *"Education at all levels"* (Respondent 55, Male, Victoria University). This succinct recommendation captures the idea that cybersecurity education should begin early and continue throughout students' academic careers, building knowledge progressively rather than delivering it in a single session.

The curriculum integration theme reflects students' understanding that cybersecurity is not a topic that can be covered once and mastered—it requires ongoing, scaffolded learning that develops increasingly sophisticated understanding over time.

✓ *Awareness Campaigns and Sensitization*

Twenty-eight respondents (17.7%) called for awareness campaigns and sensitization programs to reach students through multiple channels. This theme emphasizes broad, ongoing communication rather than formal instruction.

A respondent from Victoria University recommended multi-channel awareness building: *"Creating mass awareness about risks that expose people to cyber security threats. Sensitize students to create awareness"* (Respondent 100, Female, Victoria University; Respondent 108, Male, Victoria University). The phrase "mass awareness" suggests the student envisions campaigns reaching all students, not just those who opt into training.

Another student emphasized the continuous nature of awareness efforts: *"Continuous sensitizing of students about the various cyber security threats"* (Respondent 158, Female, Victoria University). The word "continuous" is significant—it reflects understanding that one-time awareness campaigns are insufficient as threats evolve and new students join the community.

A respondent from Cavendish University connected awareness to specific learning objectives: *"Sensitising them about the existence, effects and prevention of cybersecurity threats"* (Respondent 120, Female, Cavendish University). This three-part framework—existence (awareness that threats exist), effects (understanding of consequences), and prevention (knowledge of countermeasures)—provides a useful structure for designing awareness content.

The awareness campaigns theme reflects students' recognition that different learning styles and preferences require multiple communication channels. Formal training reaches some students, but ongoing awareness messaging through posters, emails, social media, and events can reinforce key messages and reach those who may not attend structured programs.

✓ *Practical and Hands-On Training Sessions*

Eighteen respondents (11.4%) specifically requested practical, hands-on training rather than purely theoretical instruction. This reflects students' desire for applicable skills they can immediately use, rather than abstract principles they may struggle to translate into action.

A respondent from Victoria University articulated this preference with notable clarity: *"There should be more practical sessions and simulations tailored to fit every student even those who are not into I.T course. Also more emphasis on how we can recover devices or accounts once they have been compromised"* (Respondent 26, Male, Victoria University). This recommendation makes two important points: practical sessions should be accessible to non-technical students (tailored to their needs and backgrounds), and content should include remediation skills (recovery after compromise) not just prevention. The focus on "how we can recover" suggests this student values resilience—the ability to respond effectively when prevention fails.

Another student recommended using real incidents as teaching tools: *"Hands on information. Use real and actual cyber security incidents to illustrate the impact of cyber threats and discuss steps to mitigate them"*

(Respondent 37, Female, Ndejje University; Respondent 125, Male, Cavendish University). The emphasis on "real and actual" incidents reflects students' desire for authentic learning experiences that demonstrate threats' real-world consequences.

A respondent from Cavendish University offered a memorable principle for effective education: *"Carry out engaging activities to educate people, other than just talking to people. 'Actions speak louder than words'"* (Respondent 134, Female, Cavendish University). The proverbial conclusion captures the essence of the hands-on learning preference—students want to do, not just hear.

The practical training theme reflects students' recognition that cybersecurity is ultimately about behavior, not just knowledge. They seek educational experiences that build skills and habits, not just awareness.

✓ *Mandatory or Compulsory Training*

Fifteen respondents (9.5%) advocated for making cybersecurity training mandatory for all students, recognizing that voluntary programs may not reach those who need them most—including the 3.8% who admitted taking no protective measures.

A respondent from Victoria University proposed an innovative approach linking training to platform access: *"The universities or social media platforms should make it compulsory for users to go through a mandatory sensitization or training of cybersecurity threats before the user signs up or account gets approved"* (Respondent 27, Male, Victoria University). This recommendation suggests using account creation as a teachable moment—requiring demonstrated awareness before granting access. While potentially controversial, this approach reflects the student's recognition that voluntary training may not reach those who most need it.

Another student emphasized universality with simple clarity: *"Making it a must to teach students on how to safeguard themselves from those attacks. Making the training a must"* (Respondent 38, Male, Ndejje University; Respondent 97, Male, Victoria University). The repetition of "making it a must" emphasizes the student's conviction that optional training is insufficient.

A respondent from Cavendish University suggested universal coverage without specifying compulsory mechanisms: *"At least have a training for each student about cyber security"* (Respondent 139, Female, Cavendish University). The phrase "each student" captures the universal aspiration—every student should receive some cybersecurity education, not just those who self-select.

The mandatory training theme reflects students' understanding that cybersecurity is not an optional luxury but a necessary competency for modern life, and universities have a responsibility to ensure all graduates possess basic protective knowledge.

✓ Platform Security Features and Improvements

Fourteen respondents (8.9%) directed recommendations at social media platforms, calling for improved security features, better default settings, and more effective user education within platforms.

A respondent from Victoria University provided exceptionally detailed and insightful recommendations for platform improvement: *"Social Media Platforms: Stop hiding security settings. Use pop-ups that are impossible to ignore to guide us through privacy checkups and warn us about suspicious messages. Gamify it with badges for securing our accounts. Protect us by default, don't make us dig for it"* (Respondent 49, Male, Victoria University).

This response demonstrates sophisticated understanding of user experience design principles. The recommendation to "stop hiding security settings" addresses the common problem where important controls are buried in menus, making them inaccessible to average users. The suggestion to use "pop-ups that are impossible to ignore" recognizes that subtle notifications are easily overlooked—effective guidance may require more intrusive design. The gamification idea—using badges as incentives and recognition for security behaviors—draws on behavioral economics principles to motivate positive actions. The concluding principle—"Protect us by default, don't make us dig for it"—captures the fundamental insight that security should be the default state, not an opt-in configuration requiring user effort.

Another student recommended using platform advertising resources for education: *"Instead of showing ads related to useless information, they should make ads about awareness and educating ads"* (Respondent 85, Male, Victoria University). This creative suggestion recognizes that platforms already have advertising infrastructure that could be repurposed for public education.

A respondent from Cavendish University offered recommendations spanning multiple improvement areas: *"Social media platforms should make security settings easier to understand and send alerts about potential threats or suspicious logins. They can also run short awareness campaigns targeting young users about privacy, password safety, and recognizing online scams"* (Respondent 143, Female, Cavendish University). This response addresses interface design (easier settings), proactive notification (threat alerts), and targeted education (awareness campaigns)—a multi-faceted approach to platform-led security.

The platform improvement theme reflects students' recognition that individual behavior change, while important, is insufficient without platform-level changes that make security easier and more intuitive. Students are calling for shared responsibility between users and platforms.

✓ Regular and Continuous Training Programs

Twelve respondents (7.6%) emphasized that training should be ongoing rather than one-time events, recognizing that threats evolve continuously and that knowledge needs reinforcement.

A respondent from Victoria University stated this clearly: *"Continuous and persistent provision of information about cyber threats, with relevant example scenarios. Conduct continuous training"* (Respondent 58, Male, Victoria University; Respondent 156, Male, Victoria University). The words "continuous" and "persistent" appear twice, emphasizing the importance of ongoing rather than one-off education.

Another student recommended daily engagement: *"Daily cyber security awareness tips. Have regular cyber security trainings"* (Respondent 56, Male, Victoria University; Respondent 117, Male, Victoria University). "Daily tips" suggests the student values frequent, manageable information delivery over intensive but infrequent sessions.

A respondent from Cavendish University connected continuity to quality: *"Daily Trainings on Cybersecurity awareness both as open security information courses and holding high quality cybersecurity with industry experts"* (Respondent 146, Male, Cavendish University). This recommendation combines frequency (daily) with quality (industry experts), suggesting both dimensions matter.

The continuous training theme reflects understanding that cybersecurity is not a topic that can be mastered in a single session—it requires ongoing engagement as threats evolve and as students' technology use changes.

✓ Real-Life Examples and Case Studies

Eight respondents (5.1%) specifically requested training that uses real-life examples and case studies to make learning relevant and memorable. This theme reflects students' desire for concrete, relatable examples rather than abstract principles.

A respondent from Cavendish University recommended: *"Use real and actual cyber security incidents to illustrate the impact of cyber threats and discuss steps to mitigate them"* (Respondent 125, Male, Cavendish University). The emphasis on "real and actual" incidents suggests this student finds hypothetical examples less compelling or credible than authentic cases.

Another student suggested experiential learning: *"Teaching and sharing such links to students to experimental"* (Respondent 68, Male, Victoria University). While the phrasing is unclear, this appears to recommend using actual examples (possibly simulated) as experimental learning materials.

The real-life examples theme reflects students' recognition that authentic cases make threats tangible and memorable. Case studies of actual incidents—particularly

those affecting students or similar populations—can demonstrate consequences concretely and illustrate effective response strategies.

✓ *Guest Lectures and Industry Experts*

Six respondents (3.8%) recommended bringing in external experts to provide specialized knowledge and real-world perspectives that may not be available within the university.

A respondent from Cavendish University suggested: *"Holding high quality cybersecurity with industry experts"* (Respondent 146, Male, Cavendish University). The phrase "high quality" suggests this student associates external experts with elevated content standards.

The guest lecture's theme reflects students' desire for diverse perspectives and connection to professional practice. Industry experts can share current threat intelligence, career insights, and practical experience that complement academic instruction.

✓ *Use of Media (TV, Radio, Social Media Ads)*

Five respondents (3.2%) recommended using mass media and social media platforms themselves to disseminate cybersecurity education broadly.

A respondent from Victoria University suggested a multi-channel approach: *"Have lectures educating students about cybersecurity and also post on university platform give out fliers and also host lectures on radios and TVs especially on the ones commonly used by students"* (Respondent 94, Female, Victoria University). This comprehensive recommendation spans formal lectures, university platforms, printed materials (fliers), and broadcast media (radio, TV), with attention to channels students actually use.

Another student recommended leveraging platform communication capabilities: *"Send various message on social media informing users about cybersecurity"* (Respondent 101, Male, Victoria University). Using social media to deliver security education meets students where they already spend time.

The media use theme reflects understanding that effective communication requires meeting audiences through channels they already use, with messages designed for each medium's characteristics.

✓ *Strong Password Enforcement*

Four respondents (2.5%) specifically called for institutions to enforce strong password practices, suggesting that voluntary adoption may be insufficient.

A respondent from Victoria University stated with emphasis: *"Emphasize the use of strong passwords. Use strong passwords. Teach them to use strong passwords and never save them anywhere"* (Respondent 73, Male, Victoria University; Respondent 109, Male, Victoria University; Respondent 113, Female, Victoria University). The repetition and the final prohibition

("never save them anywhere") suggest this student holds strong views about password practices, though the advice to never save passwords conflicts with password manager recommendations, indicating some confusion about optimal practices.

The password enforcement theme reflects students' recognition that some security practices may need requirements rather than recommendations to achieve universal adoption.

✓ *Free Cybersecurity Courses and Resources*

Four respondents (2.5%) requested free access to cybersecurity learning resources, recognizing that cost may be a barrier to self-education.

A respondent from Victoria University suggested: *"Free cyber security courses for all students. Provide free tutorials"* (Respondent 2, Male, YMCA; Respondent 41, Male, Ndejje University; Respondent 83, Male, Victoria University). The emphasis on "free" and "all students" reflects concern that cost should not limit access to essential knowledge.

Another student recommended using freely available resources: *"Under go some cyber security Tutorials on YouTube and also do some reading online"* (Respondent 131, Male, Cavendish University). This recommendation recognizes that valuable resources already exist freely online—universities could guide students to these materials.

The free resources theme reflects students' desire for accessible, low-barrier learning opportunities that don't require financial investment or formal enrollment.

V. DISCUSSION OF FINDINGS

➤ *Introduction*

This chapter presents a comprehensive discussion of the study's findings, interpreting the results within the context of existing literature and theoretical frameworks. The discussion integrates quantitative and qualitative data to provide a holistic understanding of cybersecurity awareness, risky behaviors, and threat experiences among Ugandan university students. Each major finding is examined in relation to previous research, with particular attention to studies conducted in developing country contexts and among similar demographic populations. The discussion concludes with theoretical implications, practical recommendations, and reflections on the study's contributions to knowledge.

➤ *Social Media Platform Usage Among University Students*

• *WhatsApp Dominance and Its Implications:*

The finding that 96.9% of students use WhatsApp "Often" or "Very Frequently," with zero respondents reporting never using the platform, represents a level of market penetration rarely seen in technology adoption studies. This near-universal adoption positions WhatsApp

as the primary digital environment where Ugandan university students live, communicate, and conduct their online lives. The platform's dominance exceeds global averages and reflects deeper patterns of digital integration in the East African context.

Several factors explain WhatsApp's supremacy in this population. The platform's end-to-end encryption, while privacy-protecting, creates what might be termed a "digital fortress" where communications occur beyond the visibility of authorities and platform moderators. This characteristic, combined with low data consumption relative to competitors, makes WhatsApp particularly suited to the Ugandan context where mobile data costs remain significant. Students use WhatsApp not merely as a social platform but as an infrastructure for academic life—class groups, assignment discussions, lecture notifications, and peer collaboration all flow through WhatsApp channels.

The cybersecurity implications of this dominance are profound. Attackers naturally concentrate where potential victims congregate, making WhatsApp the primary vector for phishing attempts, account compromises, and social engineering attacks targeting students. The qualitative findings confirm this concentration, with numerous respondents describing WhatsApp-based threats including hacked accounts used to target contacts, suspicious links shared in groups, and impersonation attempts via the platform.

Recent research on phishing susceptibility among young adults provides important context for understanding this vulnerability. [19] found that traditional factors linked to phishing susceptibility, such as training and prior experience, did not predict how securely users handled SMiShing (SMS phishing) messages. Even users who reported receiving phishing training exhibited risky behaviors when confronted with text-based attacks. This suggests that WhatsApp's centrality in student communication may actually increase vulnerability by creating familiarity that attackers can exploit—users let their guard down in environments they associate with trusted contacts and routine communication.

The convergence of high platform concentration, limited security training, and the unique characteristics of mobile-based attacks creates a perfect storm of vulnerability. Students spend hours daily in an environment where they are regularly exposed to potential threats, yet most lack the sophisticated threat literacy needed to distinguish legitimate communications from sophisticated attacks. This finding aligns with the Uganda Communications Commission's (2023) report indicating over 90% WhatsApp penetration among Ugandan youth, confirming that the platform has become deeply embedded in the social fabric of university life.

- *TikTok's Ascendancy and Visual Platform Risks:*

TikTok's emergence as the second most frequently used platform, with 59.5% of students using it often or

very frequently, represents a significant shift in student digital engagement toward entertainment-focused, visually-oriented content. This finding aligns with global trends showing Gen Z's preference for short-form video content and creative self-expression platforms over text-based social networking [3].

The cybersecurity implications of TikTok's popularity differ from those of WhatsApp. TikTok's emphasis on video content, trends, and challenges exposes students to different threat vectors, including malicious challenges that encourage harmful behaviors, inappropriate content algorithmically recommended to minors, and data privacy concerns related to the platform's ownership structure. The visual nature of the platform also creates unique opportunities for image-based abuse, where personal videos can be downloaded, altered, or redistributed without consent.

Gender differences in TikTok usage revealed in this study—with 52.2% of female students using it very frequently compared to 31.3% of males—suggest that female students may face disproportionate exposure to platform-specific risks. Research on social media privacy concerns has documented that female users often express greater concern about image-based risks and unauthorized sharing of personal content [1]. This gender dimension requires targeted intervention approaches that address the specific threat landscape different student groups navigate.

The rapid rise of TikTok among university students also highlights the challenge of keeping cybersecurity education current. Platforms that did not exist a decade ago now dominate student attention, yet educational curricula often lag behind these shifts. Students receive training based on threat models from previous technological eras while navigating contemporary platforms with novel risk profiles. [15] documented similar challenges in their study of digital literacy among Ugandan university students, noting that curriculum development struggles to keep pace with technological change.

- *Facebook's Declining Relevance and Platform Migration Patterns:*

The finding that only 17.1% of students use Facebook often or very frequently, with 23.4% never using it, confirms global trends of youth migration away from the platform [3]. This exodus has important implications for threat exposure and cybersecurity education. Students who have abandoned Facebook may assume they are less exposed to online threats, creating a false sense of security while remaining highly active on WhatsApp and TikTok, which present their own unique risks.

The platform migration pattern also complicates threat detection education. Students who learned to identify phishing attempts on Facebook may not recognize equivalent threats on TikTok or WhatsApp, where attack vectors differ. Research on SMiShing has demonstrated

that phishing detection skills do not automatically transfer across communication channels [19]. Users must develop channel-specific threat literacy, yet current educational approaches rarely address this need.

- *Gender-Based Platform Preferences and Targeted Vulnerabilities:*

The striking gender disparities revealed in platform preferences—particularly Snapchat's strong female bias (only 13.0% of females never use it compared to 47.3% of males)—demonstrate that cybersecurity interventions must be gender-sensitive, addressing the specific platforms and usage patterns of different student groups. Female students' higher engagement with visually-oriented platforms may expose them to different threats (image-based abuse, stalking, appearance-based scams) compared to male students' more balanced platform distribution.

This finding aligns with research showing that women often report higher levels of concern about privacy and online safety, yet may also engage more intensively with platforms that create particular vulnerabilities [8]. The tension between platform benefits and risks is not gender-neutral, and interventions must acknowledge these differential exposure patterns.

The gender differences also suggest that peer-led security education might benefit from gender-specific approaches. Female students' higher engagement with Snapchat and TikTok creates opportunities for platform-specific safety messaging delivered through channels and in formats that resonate with their usage patterns. Male students' slightly higher engagement with Twitter and Telegram suggests different communication channels for reaching that population.

➤ *Risky Social Media Behaviors*

- *Public Sharing of Personal Identification Information:*

The finding that 67.1% of students publicly share their real names and birth dates represents what can only be described as a foundational security vulnerability. This behavior directly contradicts basic cybersecurity principles and provides attackers with precisely the information needed for identity theft, security question answers, and targeted social engineering.

The prevalence of this behavior must be understood within its cultural context. In many Ugandan communities, online authenticity—using real identities to build trust and maintain connections—is socially valued. Students may perceive privacy-seeking behavior as suspicious or antisocial. This cultural norm conflicts directly with security best practices, creating a tension that requires nuanced intervention. Simply telling students to stop sharing information is unlikely to succeed when social pressures push in the opposite direction.

Research on cybersecurity awareness among Gen Z students in developing countries has documented similar patterns. A study of Bangladeshi university students found

that cultural factors significantly influenced information sharing behaviors, with students prioritizing social connection over privacy concerns [20]. The researchers concluded that effective interventions must address the social benefits students derive from sharing, not merely the risks.

The qualitative findings in this study provide insight into students' reasoning. Several respondents described limiting personal information sharing as a protective measure, demonstrating awareness of the risks. However, the gap between this awareness (11.4% mentioned privacy practices) and actual behavior (67.1% share names and birth dates) suggests that knowledge alone does not drive behavior. Students navigate complex trade-offs between security and social connection, often prioritizing immediate social benefits over distant, probabilistic security risks.

This finding aligns with research in [2] who found that student perceptions of social engineering attacks often underestimate the value of seemingly innocuous personal information. Students do not recognize that their birth date, combined with publicly available name, can enable attackers to answer security questions, impersonate them to contacts, or build convincing phishing narratives.

- *Password Reuse and the Convenience-Security Trade-off:*

Password reuse by 58.2% of students represents another critical vulnerability with cascading consequences. This finding aligns with global research documenting password reuse as one of the most persistent cybersecurity challenges ([12], [2]). The cognitive burden of managing multiple unique passwords leads users to prioritize convenience over security, assuming—often incorrectly—that their accounts are not valuable enough to target.

The qualitative data enriches understanding of this behavior. Students who described using strong passwords (39.2%) often focused on password complexity rather than uniqueness. A password can be complex yet reused across dozens of accounts, providing minimal protection if any single account is compromised. This suggests that students have internalized messaging about password strength while missing the equally important principle of password uniqueness.

The cascading risk of password reuse—where one compromised credential leads to multiple account takeovers—appears poorly understood by students. When attackers obtain credentials from a low-value account breach, they systematically test those credentials against email, banking, and major social media platforms [4]. Students who reuse passwords across accounts effectively create a single point of failure for their entire digital identity.

Recent research on cyber hygiene has questioned whether traditional password advice remains appropriate for contemporary users. [21] developed the Cyber

Hygiene Inventory (CHI), a validated measure of security behaviors, and found that traditional password practices were inconsistently related to overall security posture. This suggests that password behaviors may be influenced by factors beyond knowledge and intention, including platform design, default settings, and the availability of password management tools.

- *Positive Link-Clicking Behavior and Message Effectiveness:*

The finding that 80.4% of students rarely or never click unverified links represents the most positive security behavior among all measured practices. This suggests that basic "don't click suspicious links" messaging has been remarkably effective, likely due to its simplicity, memorability, and consistent reinforcement across multiple channels.

This success offers important lessons for cybersecurity education. The link-clicking message is simple, actionable, and can be applied without technical expertise. It provides a clear rule that students can follow even when they don't fully understand the underlying threat mechanisms. This contrasts with password guidance, which has become increasingly complex (length, complexity, uniqueness, regular changes, password managers) and may overwhelm users.

The qualitative findings reinforce this. Students described link caution using simple, absolute terms: "I don't click in links that I don't know the source," "Avoiding at all times clicking on links from unknown sources." The rule-based approach appears to have been internalized as a habit rather than a conscious decision requiring ongoing evaluation.

However, the 19.6% who sometimes or often click unverified links remain vulnerable, particularly to sophisticated phishing attacks that create convincing pretexts for link-clicking. Research on phishing susceptibility has documented that overconfidence in detection ability actually increases vulnerability, as users who believe they can identify phishing attempts may engage with suspicious content they would otherwise avoid [22]. This "security expertise bias" suggests that a subset of students may be at elevated risk precisely because they believe they are immune. [23] found similar patterns in their study of scam protective behaviors among college students, noting that those with higher self-reported confidence were not necessarily better at avoiding scams. The current study's findings extend this research to the Ugandan context, confirming that the confidence-competence gap is a cross-cultural phenomenon.

- *Acceptance of Unknown Friend Requests:*

The finding that 47.9% of students accept friend requests from unknown persons at least sometimes reflects the tension between social openness and security that characterizes much of online behavior. University students, particularly first-years, may accept unknown requests to expand their social networks, find academic

connections, or simply out of politeness. The social norms of platform use—where accumulating connections is often encouraged and viewed positively—conflict directly with security considerations.

This behavior creates direct pathways for malicious actors to access personal information and build trust for subsequent attacks. Attackers who establish connection through accepted friend requests gain access to whatever information the user shares with connections, can observe posting patterns to identify optimal targeting moments, and can build relationship capital that makes subsequent phishing attempts more credible.

The relatively low mention of rejecting unknown requests as a protective measure (7.6%) compared to the prevalence of the risky behavior suggests that many students do not recognize connection requests as a significant threat vector. This represents an opportunity for education that reframes connection acceptance as a security decision rather than a social courtesy.

Research on social engineering has documented how attackers exploit this gap. [12] found that fake profiles with compelling narratives build connections over weeks or months before launching attacks, leveraging the trust established through accumulated interactions. Students who accept unknown requests are not just exposing themselves to immediate risk but potentially planting seeds for future attacks.

➤ *Cybersecurity Threat Exposure*

- *Phishing Prevalence and Detection Challenges:*

The finding that 35.4% of students have experienced phishing attempts confirms social media platforms as primary vectors for social engineering attacks targeting university students. This rate exceeds findings from some regional studies [7] and suggests that Ugandan students are heavily targeted by cybercriminals. The discrepancy between high self-reported phishing understanding (63.2%) and actual exposure rates suggests either overconfidence in detection abilities or successful attacks that bypass detection.

The qualitative accounts of phishing attempts provide rich insight into how these attacks manifest. Students described receiving messages promising free shopping vouchers, job opportunities, and online course access—classic phishing lures exploiting psychological triggers of greed, need, and curiosity. More sophisticated attempts involved compromised friend accounts, adding credibility through trusted sources.

One respondent's account is particularly instructive: *"I one time received a message in a WhatsApp group when my friend was hacked and I tapped into a certain UNICEF link and this guy was like send me money... After he gave me an offer to give me that recharge money but he didn't know I had a two-step verification code in my account. After him reaching that step, he asked for it and I rejected his request and thereafter he gave up."* This narrative

illustrates how 2FA can block attackers even after users engage with malicious content—a powerful testament to layered security.

Recent research on SMiShing has revealed that traditional predictors of phishing susceptibility do not necessarily apply to text-based attacks [19]. Factors such as training, prior experience, and demographic characteristics that predict email phishing vulnerability may not translate to SMS and messaging app contexts. This suggests that the 35.4% phishing exposure rate may actually underrepresent the problem, as students may encounter threats they do not recognize as such.

The finding that 27.2% of students reported no threat experiences, despite 35.4% reporting phishing attempts in the quantitative section, supports this. Some students are likely encountering threats without recognizing them, remaining vulnerable precisely because they do not know what to look for. This aligns with research by [1], who found that only 23% of students could correctly identify phishing attempts despite higher self-reported awareness.

- *Account Hacking and Identity Theft:*

The 21.5% account hacking rate and 20.9% identity theft rate represent substantial victimization levels with serious consequences for affected students. These rates are concerning but consistent with regional studies in East Africa, where cybersecurity protections may be less developed than in high-income countries ([12], [10]).

The qualitative accounts reveal the human impact behind these statistics. One respondent described losing a TikTok account with 40,000 followers and receiving no response from platform support, leading them to abandon the platform entirely. This represents not just inconvenience but destruction of digital property and social capital built over time. The emotional impact is evident: "This made me leave TikTok for good and forever."

Another respondent described cascading consequences affecting their social network: "That time my WhatsApp was hacked and I was logged out and I couldn't access my account and they started sending messages to my contacts. But all I did was to report stolen account and it was instantly blocked and given 30 days before I can access it again." This account reveals a critical gap in platform recovery mechanisms. The 30-day lockout period leaves victims unable to warn contacts while attackers continue exploiting their identity.

The convergence of password reuse (58.2%), public information sharing (67.1%), and account hacking (21.5%) suggests a causal chain that, while not achieving statistical significance in this study, aligns with cybersecurity theory. Attackers can assemble personal information from public profiles, attempt credentials exposed in previous breaches, and exploit password reuse to access multiple accounts. Each risky behavior contributes incrementally to overall vulnerability.

Research by [8] found similar patterns among Palestinian university students, where risky online behaviors were significantly associated with cybercrime victimization. Their study documented that students who engaged in multiple risky behaviors faced substantially higher odds of experiencing account compromise, identity theft, and financial cybercrime.

- *Malware and Technical Threats:*

The finding that 15.2% of students have experienced device malware via social media, while lower than other threat categories, remains concerning given the potential for malware to spread to institutional networks. Students' devices connecting to university Wi-Fi could introduce malware that compromises broader institutional security, highlighting how individual student behaviors can create organizational risks.

The relatively low prevalence of malware compared to phishing and hacking may reflect the mobile-first nature of students' internet access. Mobile operating systems have stronger application sandboxing and permission controls than traditional desktop environments, potentially reducing malware infection rates. However, mobile-specific threats including malicious apps, SMS-based attacks, and operating system vulnerabilities present their own risk profile.

Research on SMiShing has noted that mobile devices' limited screen real estate makes it more difficult for users to scrutinize messages for phishing indicators [22]. URLs may be truncated, sender information may be hidden, and security indicators that would be visible on desktop may not appear. This creates a systematically higher vulnerability profile for mobile users, who constitute the majority of the student population in this study.

➤ *The Training Gap: A Foundational Failure*

- *Magnitude and Implications of the Training Gap:*

The finding that nearly 60% of students lack clear recollection of cybersecurity training represents what may be the single most important finding of this study. Only 41.8% of students agreed or strongly agreed they had received cybersecurity awareness training, while 37.4% disagreed or strongly disagreed, and 20.9% were uncertain. This means that a majority of students cannot recall ever being formally educated about online safety.

This finding directly validates the problem statement's assertion that cybersecurity education is not systematically integrated into higher education curricula in Uganda. Despite national frameworks including NITA-U and [10], and despite institutional ICT policies at the participating universities, students are not receiving the behavioral training necessary to protect themselves online. The gap between policy and practice appears substantial.

The training gap explains many of the risky behaviors and threat exposures documented in this study.

Students cannot practice what they have not been taught. They cannot recognize threats they have never learned to identify. They cannot adopt protective measures they have never heard about. The training gap is not merely one finding among many—it is the foundational deficit from which other vulnerabilities flow.

Research on cybersecurity education in developing countries has documented similar patterns. A study of Gen Z university students in Bangladesh found that formal cybersecurity education was rare, with most students relying on informal learning through peers, media, and personal experience [20]. The researchers concluded that institutional education gaps create systematic vulnerability across entire student cohorts.

The qualitative findings reinforce this: Students who described sophisticated protective measures often mentioned specific training experiences or personal backgrounds in computing. Those who took no measures expressed complete unfamiliarity: "I have no idea what this is about. I hadn't thought about it before." The training gap creates a two-tiered student population—those who have learned security somewhere (formal education, personal interest, peer knowledge) and those who navigate online spaces entirely unprotected. [15] documented similar patterns in their study of digital literacy at Makerere University, finding that students who had received formal ICT training demonstrated significantly higher cybersecurity awareness than those who had not. Their research concluded that institutionalizing cybersecurity education across all disciplines, not just computing programs, is essential for building a digitally resilient student population.

- *The Confidence-Competence Gap:*

The finding that 79.8% of students feel confident protecting their accounts, despite limited training and demonstrated risky behaviors, represents what psychologists term the Dunning-Kruger effect—a cognitive bias wherein individuals with limited competence overestimate their abilities. This overconfidence creates a dangerous psychological vulnerability that compounds the training gap.

Students who believe they are already competent see no reason to seek training or adopt new protective measures. They may engage with suspicious content precisely because they believe they can identify threats, when in fact their detection abilities are underdeveloped. Research on phishing detection has documented that overconfident users are actually more susceptible to attacks, as they let down their guard based on inflated self-assessment ([22], [23]).

The qualitative findings provide striking illustrations of this gap. Students who described comprehensive security practices demonstrated sophisticated understanding. But the aggregate data reveals a population that feels far more capable than their behaviors warrant. This suggests that cybersecurity interventions must first address the awareness gap—helping students recognize

what they do not know—before attempting to change behavior.

Recent research on SMiShing vulnerability has identified a related phenomenon termed "security expertise bias" [19]. Participants with higher levels of security training and awareness were actually less accurate in identifying legitimate messages, suggesting that expertise can create overconfidence that undermines careful scrutiny. This finding complicates the training picture, suggesting that how students are trained matters as much as whether they are trained. [1] found that personal characteristics significantly influenced phishing awareness and avoidance behavior, with overconfident individuals demonstrating lower actual detection rates. Their research emphasizes that effective cybersecurity education must calibrate students' self-assessment, not just transmit information.

- *Two-Factor Authentication: Progress and Gaps:*

The finding that 54.4% of students use two-factor authentication consistently represents a bright spot in an otherwise concerning picture. This relatively high adoption rate likely reflects platform defaults and requirements rather than proactive student behavior—many platforms now encourage or require 2FA, making it the path of least resistance during account setup.

However, the 32.3% who use 2FA only "Sometimes" and the 13.3% who do not use it at all represent significant security gaps. Inconsistent application means that students may enable 2FA on primary accounts (email, main social media) while leaving secondary accounts unprotected. Attackers often target these less-protected accounts precisely because they provide entry points to the user's digital ecosystem.

The qualitative data shows that some students understand 2FA's value: "Using two-factor authentication is the way to go." The gap between this understanding and consistent implementation suggests that education alone is insufficient. Default settings, platform requirements, and frictionless adoption pathways may be more effective than awareness campaigns at driving 2FA adoption.

Research on cyber hygiene has emphasized that security behaviors are shaped by environmental factors as much as individual knowledge ([21], [24]). Students who use 2FA inconsistently may do so because platforms make it optional, because recovery mechanisms are cumbersome, or because they have experienced friction when 2FA prevented access in legitimate situations. Understanding these barriers is essential for designing effective interventions.

➤ *Practical Significance and Risk Differentials*

The risk differentials observed in this study are practically meaningful and align with cybersecurity theory. Students who "Always" reuse passwords faced a 2.35-fold higher hacking rate (39.3%) compared to those who "Never" reuse passwords (16.7%). Students who "Always" accept unknown friend requests faced a 2.2-fold

higher impersonation rate (30.8%) compared to those who "Never" accept unknown requests (13.9%).

These differentials matter for intervention targeting. Even if statistical significance was not achieved in this sample, the pattern suggests that reducing password reuse and unknown request acceptance would likely reduce threat exposure. Universities cannot wait for definitive statistical proof before acting—they must base interventions on the best available evidence, which clearly points toward behavioral risk factors.

The finding that 50.0% of students who "Sometimes" click unverified links experienced phishing attempts, compared to 34.6% of those who "Never" click links, represents a 44% relative increase in risk. This pattern, while not statistically significant in this study, is consistent with the broader literature ([8], [2]) and supports continued emphasis on link caution in security education.

➤ *Connection to Theoretical Framework: Protection Motivation Theory*

- *Perceived Severity and Threat Appraisal:*

Protection Motivation Theory (PMT), developed by [14], posits that protective behavior is driven by threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy and self-efficacy). The findings of this study provide empirical support for applying PMT to cybersecurity behavior in the Ugandan university context, while also revealing important limitations.

The finding that 79.8% of students feel confident protecting their accounts suggests that perceived severity of cyber threats may be low. Students who have not experienced serious incidents, or who have experienced incidents without severe consequences, may not appreciate the potential impact—financial loss, reputational damage, academic disruption, psychological distress. This low perceived severity reduces motivation to adopt protective behaviors.

The qualitative accounts of students who experienced serious consequences provide contrast. The student who lost a 40,000-follower TikTok account described permanent platform abandonment—a severe outcome by any measure. Students who described cascading consequences affecting their contacts demonstrated heightened awareness of threat severity. These experiences appear to have shaped threat appraisal in ways that influenced subsequent behavior.

Research applying PMT to cybersecurity has documented that perceived severity is consistently associated with protective intentions [23]. Students who understand that account compromise can lead to real-world harm—financial scams targeting their contacts, identity theft affecting their credit, reputational damage limiting opportunities—are more likely to adopt protective measures. The training gap documented in this

study means that many students lack the knowledge base for accurate severity assessment.

- *Perceived Vulnerability and Optimism Bias:*

The "it won't happen to me" bias appears strongly operative in this population. Despite 35.4% phishing exposure and 21.5% hacking rates, most students feel confident, indicating they view themselves as less vulnerable than peers or believe their behaviors protect them sufficiently. This optimism bias, well-documented in health psychology and increasingly recognized in cybersecurity research, reduces protection motivation by creating a false sense of immunity.

The qualitative data reveals this bias in students who described taking few protective measures yet expressed confidence. The student who used "1234567" as a password presumably believes this is adequate protection, despite all evidence to the contrary. This disconnect between actual vulnerability and perceived invulnerability represents a critical intervention target.

Research on phishing detection has documented that overconfidence is systematically associated with poorer detection performance [22]. Students who believe they can identify phishing attempts actually perform worse than those who express uncertainty, because overconfidence leads to less careful scrutiny. This suggests that interventions must address not just knowledge but calibration—helping students develop accurate assessments of their own abilities.

- *Response Efficacy and Self-Efficacy:*

Students' inconsistent adoption of protective measures (e.g., 32.3% sometimes using 2FA) may reflect doubts about whether these measures are effective. Students who have experienced threats despite using some protections may question whether additional measures matter. Those who have never used certain protections may not understand their value.

The qualitative data provides some evidence of response efficacy beliefs. Students who described 2FA as "the way to go" clearly believe in its effectiveness. Those who mentioned specific protections in response to threat experiences demonstrated learning about what works. However, the overall pattern suggests that many students lack strong response efficacy beliefs, reducing motivation to adopt protective measures.

Self-efficacy—belief in one's ability to implement protective measures—appears high in this population (79.8% confidence), but this self-efficacy is not grounded in actual knowledge or consistent protective behaviors. PMT suggests that accurate self-efficacy—based on real competence—is necessary for appropriate protection motivation. Current inflated self-efficacy may actually reduce motivation to learn and adopt better practices, as students see no need for improvement.

Research applying PMT to scam protection among college students found that threat severity, response

efficacy, and self-efficacy significantly predicted protection intentions [23]. The current study's findings suggest that these PMT components are not being adequately developed through existing education and experience. The training gap represents a failure in the "coping appraisal" pathway—students cannot develop accurate threat perceptions or appropriate protective responses without adequate information and skill development.

➤ *Alignment with Recent Literature*

- *Confirming Global Patterns in Developing Country Context:*

The findings of this study align with and extend recent research on cybersecurity awareness among university students globally. The training gap documented here mirrors findings from Bangladesh, where researchers found that formal cybersecurity education was rare and most students relied on informal learning [20]. The prevalence of password reuse (58.2%) is consistent with global estimates and confirms that this behavior transcends national and cultural boundaries ([12], [2]).

The confidence-competence gap documented in this study reflects patterns observed in SMiShing research, where users overestimated their detection abilities and performed worse than expected ([19], [22]). This suggests that the Dunning-Kruger effect in cybersecurity is not culture-specific but rather a human cognitive bias that manifests across populations.

The platform dominance patterns observed—WhatsApp supremacy, TikTok's rise, Facebook's decline—align with global youth technology adoption trends [3] while reflecting the specific characteristics of the Ugandan digital environment [9]. This combination of global patterns and local specificity underscores the importance of contextually-grounded research.

- *Unique Contributions and Regional Context:*

This study makes several unique contributions to the literature. First, it provides empirical data on cybersecurity behaviors and threat exposure among Ugandan university students—a population for which such data has been limited. Previous research in East Africa has focused primarily on institutional and national cybersecurity frameworks rather than student-level behaviors and experiences ([10], [13]).

Second, the study documents the specific threat landscape students navigate, including the prevalence of WhatsApp-based attacks, impersonation, and account hacking. This granular understanding of threat vectors is essential for designing targeted interventions that address students' actual experiences rather than generic threats.

Third, the qualitative data provides rich insight into students' reasoning, decision-making, and lived experiences. The accounts of students who lost accounts, recovered from compromise, and developed sophisticated security practices illustrate the human dimensions of

cybersecurity that survey data alone cannot capture. This methodological approach aligns with calls for mixed-methods research in cybersecurity [16].

Fourth, the study's identification of the training gap as a foundational deficit has clear policy implications. Unlike behavioral patterns that may be difficult to change, the training gap can be addressed through institutional action. Universities can integrate cybersecurity into curricula, develop awareness campaigns, and ensure that all students receive basic security education. This finding supports recommendations by [15] for systematic integration of digital literacy across higher education curricula in Uganda.

- *Divergence from Some International Findings:*

While the study aligns with much international research, some divergences warrant discussion. The failure to achieve statistical significance in behavior-threat relationships contrasts with studies that have found significant associations [8], but this likely reflects sample size limitations rather than genuine differences in underlying relationships. Larger studies in other contexts have documented significant relationships between password practices and account compromise [2].

The relatively low mention of password managers and biometric authentication (5.1%) compared to studies in high-income countries reflects the different technological context. Password managers are less widely promoted in East Africa, and biometric authentication may be less available on the devices students use. This divergence highlights the importance of context-appropriate security recommendations.

The finding that 27.2% of students reported no threat experiences, despite high overall exposure rates, diverges from some international studies that have found higher threat recognition rates. This may reflect differences in threat literacy—students in contexts with more developed cybersecurity education may be better able to recognize and report threats. Alternatively, it may reflect genuine differences in threat exposure, though this seems less likely given the global nature of cyber threats [4].

VI. CONCLUSIONS

➤ *Summary of Major Findings:*

This study provides comprehensive evidence on cybersecurity awareness, behaviors, and threat exposure among Ugandan university students. The major findings can be summarized as follows:

- *Platform Usage:*

WhatsApp has achieved near-universal adoption (96.9% frequent use), making it the primary digital environment where students live and communicate. TikTok has rapidly gained prominence (59.5% frequent use), particularly among female students. Facebook continues to decline, with only 17.1% frequent use. These platform patterns shape the threat landscape students navigate and must inform targeted interventions.

- *Risky Behaviors:*

Students exhibit multiple risky behaviors that create significant vulnerabilities. Public sharing of personal identification information (67.1%) provides attackers with raw materials for identity theft and social engineering. Password reuse (58.2%) creates cascading risks where single compromises affect multiple accounts. Acceptance of unknown friend requests (47.9%) opens pathways for impersonators and scammers. Positive link-clicking behavior (80.4% cautious) represents a notable exception and suggests that simple, consistent messaging can be effective.

- *Threat Exposure:*

More than one-third of students (35.4%) have experienced phishing attempts, and approximately one-fifth have experienced account hacking (21.5%) or identity theft (20.9%). These rates confirm that social media platforms are primary vectors for cyber threats targeting university students. Qualitative accounts reveal serious consequences including loss of digital property, reputational damage, and emotional distress.

- *The Training Gap:*

The finding that nearly 60% of students lack clear recollection of cybersecurity training represents a fundamental failure in institutional preparedness. Despite national frameworks and institutional policies, students are not receiving the behavioral education necessary to protect themselves. This training gap is the single most important finding for policy and practice.

- *The Confidence-Competence Gap:*

Despite limited training and demonstrated risky behaviors, 79.8% of students feel confident protecting their accounts. This overconfidence bias creates dangerous psychological vulnerability, as students who believe they are competent see no need for improvement and may let down their guard.

- *Behavior-Threat Relationships:*

While statistical significance was not achieved, the data show directional patterns consistent with cybersecurity theory. Students who always reuse passwords face 2.35 times higher hacking risk; those always accepting unknown requests face 2.2 times higher impersonation risk. These differentials are practically meaningful and support continued emphasis on behavioral interventions.

➤ *Theoretical Implications:*

The findings support the application of Protection Motivation Theory [14] to cybersecurity behavior in the Ugandan context while highlighting important considerations. The training gap represents a failure in the coping appraisal pathway—students cannot develop accurate threat perceptions or appropriate protective responses without adequate information. The confidence-competence gap reveals that self-efficacy, a key PMT component, must be grounded in actual competence to motivate appropriate protection.

The study also reveals the limitations of individual-level behavioral models in contexts where environmental factors—platform design, default settings, institutional policies—powerfully shape security outcomes. Students' recommendations for platform improvements ("Protect us by default, don't make us dig for it") reflect sophisticated understanding that individual behavior change must be supported by environmental design. This aligns with socio-ecological approaches to cybersecurity that consider multiple levels of influence on behavior [24].

➤ *Recommendations for Policy and Practice:*

Based on these findings, the following recommendations are offered:

- *For Universities:*

- ✓ Integrate cybersecurity into curricula across all disciplines, not just computing programs. Every graduate should possess basic digital safety competencies [15].
- ✓ Develop mandatory cybersecurity training for all incoming students, delivered during orientation and reinforced throughout the academic journey.
- ✓ Use practical, hands-on training methods including simulations, case studies, and interactive exercises rather than lectures alone [23].
- ✓ Address the confidence-competence gap by helping students calibrate their self-assessment through feedback and testing.
- ✓ Leverage peer education by training knowledgeable students to support others, as documented in qualitative accounts of students helping friends.

- *For Social Media Platforms:*

- ✓ Make security the default by enabling protective features automatically rather than requiring users to find and enable them.
- ✓ Simplify security settings and make them accessible through intuitive interfaces.
- ✓ Provide in-context education through pop-ups, alerts, and guided checkups that reach users when they need security information.
- ✓ Improve account recovery mechanisms to reduce the 30-day lockout periods that leave victims unable to warn contacts.

- *For Policymakers:*

- ✓ Develop national cybersecurity education standards for higher education institutions [13].
- ✓ Support research on cybersecurity behaviors in the Ugandan context to build evidence for interventions.
- ✓ Fund awareness campaigns that reach students through channels they actually use, including social media platforms.

➤ *Study Limitations and Future Research:*

This study has several limitations that should inform interpretation of findings. The sample, while adequate for descriptive analysis, was underpowered for detecting

behavior-threat relationships. The overrepresentation of first-year students and male respondents may limit generalizability. Self-reported data may be subject to social desirability and recall biases [18].

Future research should address these limitations through larger samples, more diverse institutional representation, and longitudinal designs that track behavior change over time. Behavioral measures (simulated phishing exercises, account monitoring) could complement self-report data. Qualitative research could explore the cultural and social factors that shape security decisions in greater depth.

Despite these limitations, the study makes important contributions to understanding cybersecurity among Ugandan university students and provides an evidence base for intervention design. The findings confirm that students face serious threats, engage in risky behaviors, and lack the training necessary to protect themselves. Addressing this training gap is an urgent priority for universities, policymakers, and platforms serving this vulnerable population.

REFERENCES

- [1]. S. Alqahtani and P. Nanda, "Effects of personal characteristics on phishing awareness, anti-phishing tool usage, and phishing avoidance behavior," *IEEE Access*, 2024.
- [2]. C. J. Yap, R. C. D. Cruz and K. A. Soberano, "Student perceptions of social engineering attacks: A survey-based analysis," *Global Advances in Security Studies*, 2025.
- [3]. Statista, "Statistics: Statista," Statista, January 2023. [Online]. Available: <https://www.statista.com/statistics/1658762/share-of-active-users-on-social-networks-worldwide-by-country/>. [Accessed 11 March 2026].
- [4]. S. Morgan, *Cybersecurity Ventures*, 13 November 2020. [Online]. Available: <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>. [Accessed 11 March 2026].
- [5]. N. T. Madathil, M. Alalawi and S. K. Darota, "Evaluating and boosting cybersecurity awareness with an AI-integrated mobile app," in *IEEE Frontiers*, 2024.
- [6]. INTERPOL, "Africa Cyberthreat Assessment Report," 2022.
- [7]. A. Tadesse, "Cybersecurity awareness and social media behavior among university students in Nigeria," *African Journal of Information Systems*, vol. 12, no. 2, pp. 33-45, 2020.
- [8]. M. Ahmead, N. El Sharif and I. Abuiram, "Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross-sectional study," *Crime Science*, vol. 13, no. 1, pp. 1-13, 2024.
- [9]. Uganda Communications Commission, "Annual Market Performance Report 2022/23," 2023.
- [10]. National Information Technology Authority – Uganda, "Annual Cybersecurity Incident Report," 2023.
- [11]. H. J. Hazarika, "Impact of cybersecurity breaches on social media: A case study on undergraduate students," *Alexandria: The Journal of National and International Library and Information Issues*, 2025.
- [12]. M. Madzima and P. Mvelase, "An investigation of phishing susceptibility among university students in South Africa," *African Journal of Information Systems*, vol. 14, no. 1, pp. 55-71, 2022.
- [13]. National Information Technology Authority - Uganda, "Cybersecurity Readiness and Incident Trends Report: 2022/23," 2023.
- [14]. R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93-114, 1975.
- [15]. E. Tumwesigye, F. Kabuye and J. Nabirye, "Digital literacy and cybersecurity awareness among university students in Uganda: A case of Makerere University," *Makerere Research Series*, vol. 3, no. 2, pp. 67-84, 2021.
- [16]. J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, SAGE Publications, 2018.
- [17]. R. V. Krejcie and D. W. Morgan, "Determining sample size for research activities," *Educational and Psychological Measurement*, vol. 30, no. 3, pp. 607-610, 1970.
- [18]. M. Saunders, P. Lewis and A. Thornhill, *Research Methods for Business Students*, Pearson Education, 2019.
- [19]. M. E. Edwards and J. D. Still, "Cyber hygiene of SMiShing: What they know and where they look," *Computers & Security*, 2025.
- [20]. W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N. L. Lei and X. Xu, "The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates," *Education and Information Technologies*, vol. 28, no. 1, pp. 439-470, 2023.
- [21]. A. A. Cain, M. E. Edwards and J. D. Still, "An explanatory study of cyber hygiene behaviours and knowledge," *Journal of Information Security and Applications*, vol. 42, pp. 36-45, 2018.
- [22]. C. Faklaris, "Understanding and mitigating SMiShing vulnerability: Insights from U.S. surveys and interviews," *University of North Carolina*, Charlotte, 2025.
- [23]. E. Y. Heng, A. Chou Shigeta, Z. Y. Lee and J. C. Y. Tung, "Click with caution: Investigating the antecedents of protective behaviour towards online scams among college students," *Nanyang Technological University*, Singapore, 2025.
- [24]. A. Vishwanath, L. S. Leo, P. Goh, S. Lee, M. Khader, G. Ong and J. Chin, "Cyber hygiene: The concept, its measure and its initial tests," *Decision Support Systems*, vol. 128, pp. 113-160, 2020.