MAKERERE UNIVERSITY

COLLEGE OF BUSINESS AND MANAGEMENT SCIENCES

SCHOOL OF STATISTICS AND PLANNING

AN ASSESSMENT OF FACTORS AFFECTING CYBERSECURITY AWARENESS AMONG MAKERERE UNIVERSITY STUDENTS

BY

WANI ELIJAH

23/U/18542/PS

2300718542

A DISSERATATION SUBMITTED TO SCHOOL OF STATISTICS AND PLANNING AS A REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF STATISTICS

JULY 2026

DECLARATION

I WANI ELIJAH declare that this dissertation is out of my own efforts and has not been submitted to any university or institution for any award, with work from other scholars cited and referenced. I therefore affirm it to be original.

Signature: ..... Date: 10/08/2026.

Registration Number: 23/U/18542/PS

Student Number: 2300718542

APPROVAL

This dissertation has been submitted with my approval.

Signature: ..... Date: ....10/08/2026.....

DR. Odur Benard

University Supervisor

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor for the guidance, support and the feedback throughout this research process. I also extend my appreciation to my friends, classmates and family for their continuous encouragement and moral support.

Contents

DECLARATION ii
APPROVAL iii
ACKNOWLEDGEMENT iv
ABSTRACT viii
CHAPTER ONE: INTRODUCTION 1
1.0 Introduction 1
1.1 Background to the Study 1
1.2 Problem Statement 3
1.3 Research objectives 5
1.3.1 Main Objective 5
1.3.2 Specific Objectives 5
1.4 Hypothesis 5
1.5 Scope of the Study 6
1.5.1 Geographical Scope 6
1.5.2 Content Scope 6
1.5.3 Time Scope 7
1.6 Justification of the Study 7
CHAPTER TWO: LITERATURE REVIEW 9
2.0 Introduction 9
2.1 Literature about Cybersecurity Awareness 9
2.2.1 Gender and Cybersecurity Awareness 10
2.2.2 Age and Cybersecurity Awareness 10
2.3.1 Digital Literacy and its relationship to Cybersecurity Awareness 11
2.3.2 Digital Usage patterns and it's relationship to Cybersecurity Awareness 12
2.4.1 University Cybersecurity Awareness Programs 12
2.4.2 IT support systems and technical infrastructure 13
2.5 Summary and Conclusion 14
2.6 Limitations 15
CHAPTER THREE: METHODOLOGY 17
3.0 Introduction 17
3.1 Research Design 17

3.2 Study Population 17
3.3 Sampling Technique 18
3.3.1 Sample size determination 18
3.4 Data Collection Procedure 19
3.5 DATA MANAGEMENT 20
3.5.1 Data coding 20
3.5.2 Data Cleaning 21
3.5.3 Handling Missing Data 21
3.6 DATA ANALYSIS 22
3.6.1 Preliminary Analysis 22
3.6.2 Fitting Statistical Models and Selecting the Appropriate Model 22
3.7 ETHICAL CONSIDERATIONS 24
3.8 LIMITATIONS 25
CHAPTER FOUR: RESULTS AND INTERPRETATION. 26
4.0 Introduction. 26
4.1 Normality test of the dependent variable. 26
4.2 Reliability Analysis 27
4.3 Univariate and bivariate analysis 28
4.3.1 The influence of demographic factors (age and gender) on cybersecurity awareness among students. 28
4.3.2 The relationship between year of study and cybersecurity awareness among students. 30
4.3.3 The effect of digital literacy and digital usage patterns on cybersecurity awareness among students. 31
4.3.4 The influence of institutional factors (availability of awareness programs and IT support systems) on cybersecurity awareness among students 33
4.4 Multivariate analysis of all significant variables 34
CHAPETR FIVE: DISCUSSION, SUMMARY, CONCLUSION, RECOMMENDATION OF THE STUDY FINDINGS AND AREAS FOR FURTHER RESEARCH. 37
5.0 Introduction 37
5.1 Discussion of the findings 37
5.1.1 The influence of demographic factors (age and gender) on cybersecurity awareness among students. 37

5.1.2 The relationship between year of study and cybersecurity awareness among students. 38
5.1.3 The effect of digital literacy and digital usage patterns on cybersecurity awareness among students. 39
5.1.4 The influence of institutional factors (availability of awareness programs and IT support systems) on cybersecurity awareness among students. 40
5.2 Summary. 41
5.3 Conclusion. 41
5.4 Recommendations. 42
5.5 Area for further research. 42
REFERENCES 44
APPENDIX 49

ABSTRACT

This study examined the factors affecting cybersecurity awareness among undergraduate students at Makerere University addressing a gap in cybersecurity awareness research. Using a cross-sectional survey design, data were collected from a stratified random sample of 396 students across all academic colleges, selected via Yamane's formula from an estimated population of 38,000 students. The study assessed the influence of demographic factors (age and gender), year of study, digital literacy, digital usage patterns and institutional factors (awareness programs and IT support systems) on cybersecurity awareness.

Data were analyzed using descriptive statistics, Chi-square tests and multiple linear regression. Bivariate analysis showed no significant association between age or gender and cybersecurity awareness, while year of study, digital literacy, digital usage, and institutional factors were all significantly associated with awareness. However, in the multivariate regression model (R^2 = 0.331), only digital literacy (β = 0.427), digital usage (β = 0.167), and institutional factors (β = 0.164) remained significant independent predictors; year of study lost significance once these variables were controlled for, suggesting its influence operates indirectly through digital literacy and usage.

The findings indicate that cybersecurity awareness among Makerere University students is shaped primarily by digital competence and institutional support rather than demographic characteristics or academic seniority. The study recommends integrating cybersecurity content into digital literacy curricula, promoting purposeful digital engagement, and strengthening institutional awareness programs and IT support services.

CHAPTER ONE: INTRODUCTION

1.0 Introduction

This study examines the factors affecting cybersecurity awareness among university students at Makerere University. The study focuses on three categories of factors identified in the theoretical and empirical literature as significant determinants of cybersecurity awareness: demographic characteristics including gender and age, year of study, digital literacy competencies and digital usage patterns and institutional factors encompassing university cybersecurity awareness programs, institutional security policies and IT support systems.

1.1 Background to the Study

Cybersecurity awareness refers to knowledge, attitudes and behaviours that enable individuals to recognize and respond effectively to cyber threats. Studies emphasize that cybersecurity awareness levels among university students vary widely and are influenced by several determinants. Specific knowledge areas such as password security, browser security, and safe social media practices significantly affect students' overall cybersecurity awareness levels, with social media activities showing the highest influence among studied factors (Alqahtani 2022).Additionally, research reveals that age, digital literacy, academic discipline, and prior exposure to cyber training correlate with awareness levels, with older or more technically trained students often demonstrating better understanding and safer practices (Oroni, Xianping et al. 2025).

The rapid expansion of digital technologies has significantly transformed higher education, increasing students' reliance on online platforms for learning, communication, and social

interaction (Alenezi, Wardat et al. 2023). University students engage extensively with digital systems such as learning management platforms, email services, cloud storage, and social media, creating a broad cyberspace footprint. However, this increased digital engagement also exposes students to a range of cybersecurity threats, including phishing, malware, identity theft, and online fraud, which exploit human vulnerability rather than technical weaknesses alone. Research indicates that phishing remains one of the most prevalent threats in academic communities, with students often targeted due to high online activity and insufficient security practices (Nyasvisvo and Chigada 2023). Studies also show that nearly 70% of students exposed to simulated phishing attacks click malicious links, underscoring substantial gaps in behaviour and threat comprehension (Gwenhure 2025).

Despite growing recognition of cybersecurity risks in educational environments, there remains a deficit of context-specific evidence from developing regions such as East Africa, where digital access is rapidly increasing but formal cybersecurity education and institutional training programs are limited (Niyikora 2025). Studies in related contexts reveal that students with higher digital literacy and structured awareness interventions demonstrate greater ability to identify and prevent cyber threats, suggesting that both individual capabilities and educational frameworks are critical in shaping awareness (Md Kasim et al., 2022)

Moreover, behavioural and psychological models such as the Health Belief Model are increasingly applied to explain why students choose protective online behaviours or not, showing that perceived threat severity, self-efficacy, and cues to action influence cybersecurity practices (Ng, Kankanhalli et al. 2009). However, limited research examines how these determinants interact specifically within African university populations. Consequently, there is a need to investigate the factors affecting cybersecurity awareness among university students comprehensively, including digital

usage patterns, educational exposure, and individual behavioural determinants, so as to inform effective awareness strategies and policy interventions.

1.2 Problem Statement

Globally, higher education institutions have experienced rising ransomware attacks, credential theft, and email compromise incidents. Reports such as (Adams, Benninger et al. 2019) from EDUCAUSE indicate that 74% of global data breaches such as phishing and identity-based attacks remain the top cybersecurity threats facing universities in North America and Europe. In Africa, the burden is compounded by rapid digital adoption without equivalent growth in cybersecurity education and infrastructure. The African Union has acknowledged the growing threat of cybercrime across member states, with estimated costs of over $4 billion annually, emphasizing the need for capacity building and awareness programs (Mphatheni and Maluleke 2022). However, many African universities operate in environments where cybersecurity policies are still evolving, and structured awareness training for students remains limited.

Within East Africa countries, , the expansion of internet penetration and mobile financial services over the past decade has significantly broadened the digital attack surface for university students While this growth enhances access to digital learning and financial inclusion, it also increases exposure to cyber threats such as mobile money fraud, phishing, and social engineering attacks (Afzal, Meraj et al. 2025). In Uganda, universities including Makerere University rely heavily on digital platforms for admissions, registration, academic communication, and financial transactions. Students frequently use institutional email accounts, learning management systems, mobile money services, and social media platforms, yet structured cybersecurity awareness programs are not systematically integrated into university curricula across all disciplines. Evidence from global

studies suggests that factors such as academic background, digital literacy, prior cyber-incident exposure, gender, and access to formal cybersecurity training influence awareness levels. (Tasnim, Tasnim et al. 2025)

Developed countries have implemented cybersecurity awareness campaigns, mandatory training modules, phishing simulations and institutional cybersecurity policies. However, similar comprehensive strategies are less established in many African universities. Although national frameworks such as Uganda's Computer Misuse Act (2011) and data protection regulations exist, implementation at the institutional level, particularly in universities, remains inconsistent. Empirical data comparing cybersecurity awareness levels among university students in East Africa is sparse and most available reports focus on technical vulnerabilities rather than human awareness determinants (Oroni, Xianping et al. 2025). Despite the fact that advanced cybersecurity systems have been introduced, breaches still continue to occur due to low user awareness and unsafe digital behaviours highlighting the persistent burden of human vulnerability.

Despite growing global research on cybersecurity awareness, most in Sub-Saharan Africa. Several studies have examined cyber security awareness for example (Hadlington 2017) examined risky cybersecurity behaviours among university students. Similarly, (Bada and Nurse 2019) emphasized the importance of awareness programs in improving cybersecurity behaviour. However, these studies have concentrated on technical security controls and general user behaviour in developed contexts, with limited attention to context-specific determinants therefore there remains insufficient evidence on how demographic, behavioural, educational, and institutional factors interact to influence cybersecurity awareness within Ugandan universities specifically. This limits the development of targeted, contextually relevant awareness strategies

thereby justifying the need for localized research to identify the most significant determinants affecting cybersecurity awareness among university students in Uganda.

1.3 Research objectives

1.3.1 Main Objective

To examine the factors affecting cybersecurity awareness among Makerere University students.

1.3.2 Specific Objectives

1. To determine the influence of demographic factors (age and gender) on cybersecurity awareness among students.
2. To determine the relationship between year of study and cybersecurity awareness among students.
3. To examine the effect of digital literacy and digital usage patterns on cybersecurity awareness among students.
4. To assess the influence of institutional factors (availability of awareness programs and IT support systems) on cybersecurity awareness among students.

1.4 Hypothesis

H_{01}: There is no significant difference in cybersecurity awareness between male and female university students.

H_{02}: There is no significant relationship between age and cybersecurity awareness among university students.

H_{03}: There is no significant difference in cybersecurity awareness across different years of study among university students.

H_{04}: Digital literacy has no significant effect on cybersecurity awareness among university students.

H_{05}: Digital usage patterns have no significant effect on cybersecurity awareness among university students.

H_{06}: There is no significant relationship between exposure to university cybersecurity awareness programs and cybersecurity awareness among students.

H_{07}: The availability of IT support systems has no significant influence on cybersecurity awareness among university students.

1.5 Scope of the Study

1.5.1 Geographical Scope

The study will be conducted among Makerere University students. It will not extend to other institutions or countries, academic staff and administrative personnel. The findings will apply only Makerere University students and its not a generalisation to all public or private universities

1.5.2 Content Scope

This study is confined to the examination of factors affecting cybersecurity awareness among university students. Specifically, it investigates the influence of three categories of independent variables on cybersecurity awareness as the dependent variable. The first category encompasses demographic factors namely gender and age, year of study which are examined as individual-level

characteristics that may differentially shape students' exposure to and engagement with cybersecurity knowledge. The second category comprises digital literacy and digital usage patterns including students' technicality, critical digital skills, device security practices and engagement with online platforms such as institutional email, learning management systems, social media and mobile financial services. The third category consists of institutional factors, specifically the availability and quality of university cybersecurity awareness programs, the existence and enforcement of institutional cybersecurity policies, and the accessibility and responsiveness of university IT support systems.

1.5.3 Time Scope

The study is conducted during the academic year 2024/2025, with data collection scheduled during the second semester to ensure that respondents have had meaningful exposure to the university's digital environment, institutional systems and any awareness activities organized during the academic year.

1.6 Justification of the Study

The primary justification for this study lies in the significant and demonstrable gap in empirically grounded, context-specific research on cybersecurity awareness in Ugandan and East African higher education institutions. The overwhelming majority of existing cybersecurity awareness research has been conducted in North American and Western European contexts, with findings that may not readily transfer to the socioeconomic, infrastructural, institutional, and cultural conditions that characterize universities in Sub-Saharan Africa (Hadlington 2017). Studies that do address cybersecurity in African contexts have tended to focus on national-level policy

frameworks, technical infrastructure vulnerabilities or aggregate cybercrime statistics rather than on the human and behavioural determinants of awareness at the individual and institutional levels within universities (Chigada and Madzinga 2021). This study directly addresses this gap by generating primary empirical data on the factors that shape cybersecurity awareness among undergraduate students in a leading Ugandan university.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This chapter provides examination of existing studies regarding the factors affecting cybersecurity awareness. It evaluates the theoretical and practical play of variables of the study beginning with a breakdown of the dependent variable and through the analysis of demographic, social and institutional factors. By synthesizing empirical evidence on how these factors affect cybersecurity awareness, this identifies critical gaps in the awareness study. This chapter serves to provide a solid theoretical foundation for the study while contextualizing the factors that influence the know-how with the Makerere University students.

2.1 Literature about Cybersecurity Awareness

Cybersecurity awareness is a concept that has been operationalized in various ways across the literature. At its most basic level, it refers to an individual's knowledge of cyber threats and the ability to recognize and respond appropriately to security risks (Ben-Asher and Gonzalez 2015). (Alotaibi, Furnell et al. 2023) propose a hierarchical model of cybersecurity awareness that encompasses awareness, training and education as distinct but complementary components. Awareness in this model represents the lowest tier an individual's basic recognition of security issues while education encompasses deeper understanding and the capacity for critical analysis.

Several theoretical frameworks have been employed to explain cybersecurity awareness and behavior among students. The Protection Motivation Theory (PMT) originally proposed by Rogers (1975) and later elaborated by Maddux and Rogers (1983) posits that individuals are motivated to protect themselves from threats based on their appraisals of threat severity, vulnerability and their

own capacity to respond effectively. PMT has been widely applied in cybersecurity research to explain why individuals adopt or fail to adopt protective behaviors (Tsai, Jiang et al. 2016)

2.2.1 Gender and Cybersecurity Awareness

The relationship between gender and cybersecurity awareness has been extensively investigated with most studies finding significant differences between male and female students. A large scale survey conducted by (Shillair, Cotten et al. 2015) of over 1,000 university students found that male students consistently scored higher on objective measures of cybersecurity knowledge while female students reported higher levels of subjective concern about online threats. The authors interpreted this asymmetry through the lens of gendered socialization patterns which may lead women to be more emotionally responsive to security threats while men accumulate more technical knowledge through greater engagement with technology.

A comparative study carried out by (Bhattacharya, Verma et al. 2023) of gender differences in cybersecurity awareness across five universities in the Gulf region and found that male students outperformed female peers on technical knowledge items but that no significant gender differences emerged on awareness of social engineering threats. The authors suggest that the technical dimension of cybersecurity may be particularly subject to gender-based socialization effects while non-technical threats may be more equally distributed across gender lines.

2.2.2 Age and Cybersecurity Awareness

The relationship between age and cybersecurity awareness presents a nuanced picture. While intuition might suggest that younger students, as digital natives, would possess higher levels of cybersecurity awareness, empirical evidence does not consistently support this assumption. Age

effects examined by (Hadlington and Parsons 2017) in a sample of university students found that older students those in their late twenties and above demonstrated higher levels of cybersecurity awareness than traditional-age students, potentially reflecting greater accumulated experience with the consequences of security failures. The authors suggest that life experience and exposure to real-world cyber threats may be more important determinants of awareness than age per se.

Conversely, (Sommestad, Hallberg et al. 2014) found that younger students demonstrated higher awareness of emerging threats such as mobile security risks and social media privacy, reflecting their greater familiarity with these technologies. These findings highlight the multidimensional nature of cybersecurity awareness and suggest that age effects may be domain-specific rather than universal.

2.3.1 Digital Literacy and its relationship to Cybersecurity Awareness

Digital literacy broadly defined as the ability to use digital technologies effectively, critically and safely has been theorized as a foundational prerequisite for cybersecurity awareness(Calvani, Fini et al. 2012). The conceptual overlap between digital literacy and cybersecurity awareness is significant, both constructs emphasize the importance of critical evaluation of digital information, awareness of online risks, and the capacity for informed decision-making in digital environments.

The relationship between digital literacy and cybersecurity awareness examined by (Contieri, Anholon et al. 2022) in a sample of Portuguese university students and found that digital literacy significantly predicted performance on cybersecurity knowledge assessments even after controlling for academic discipline and prior technology experience. The authors suggest that digital literacy programs in higher education should explicitly incorporate cybersecurity content to leverage the positive associations between these constructs.

2.3.2 Digital Usage patterns and it's relationship to Cybersecurity Awareness

The frequency, duration and nature of students' internet use have been examined as potential predictors of cybersecurity awareness, with complex and sometimes counterintuitive findings. An investigation by (Hadlington 2017) about the relationship between internet usage patterns and cybersecurity risk-taking behavior in a sample of UK university students, finding that higher frequency internet users demonstrated greater engagement in risky online behaviors, contrary to the hypothesis that more experienced users would develop greater caution.

The nature of online activities, rather than simple usage frequency, appears to be a more relevant predictor of cybersecurity awareness. Students who engage primarily in social media and entertainment activities demonstrate lower security awareness than those who used the internet for academic research and information seeking, suggesting that the cognitive engagement associated with different activities mediates the relationship between usage and awareness.(Workman 2007)

Mobile device usage has emerged as a particularly important dimension of digital usage patterns in the context of cybersecurity. Findings by (Mylonas, Kastania et al. 2013) suggested that university students were significantly less likely to apply security measures to their mobile devices than to desktop computers, despite using mobile devices for increasingly sensitive transactions including banking, healthcare and academic work. The authors attribute this asymmetry to a combination of perceived inconvenience, inadequate awareness of mobile security risks and a false sense of security created by app store vetting processes.

2.4.1 University Cybersecurity Awareness Programs

Institutional cybersecurity awareness programs represent the primary mechanism through which universities seek to improve students' security knowledge and behaviors. (Bulgurcu, Cavusoglu et al. 2010) conducted a study of information security policy compliance in an organizational context and found that awareness programs that effectively communicated the rationale behind security policies rather than simply issuing mandates were significantly more effective in driving compliant behavior. Applied to university settings, this finding suggests that student awareness programs should emphasize the personal relevance and institutional importance of cybersecurity rather than adopting a purely compliance-oriented approach.

Research from developing countries has highlighted additional challenges for university awareness programs, including resource constraints, inadequate technical infrastructure, and cultural factors that may influence receptiveness to security messaging. (Chigada and Madzinga 2021) found that South African university cybersecurity awareness programs were frequently under-resourced and inconsistently implemented, contributing to persistently low awareness levels among students. The authors recommend a systems-level approach that integrates cybersecurity awareness into the broader curriculum rather than relying on standalone programs.

2.4.2 IT support systems and technical infrastructure

The availability and quality of institutional IT support systems have been identified as important enabling factors for student cybersecurity awareness. A research carried out by (Al-Janabi and Al-Shourbaji 2016) surveyed students across multiple Iraqi universities and found that students who reported regular access to IT support services demonstrated higher levels of cybersecurity awareness and more consistent engagement in protective behaviors. The authors attribute this finding to both the direct educational function of IT support interactions and the indirect effect of

IT support availability on students' confidence in their ability to respond effectively to security incidents.

The role of organizational security resources including technical controls, IT infrastructure and support services in shaping security behavior examined by (Herath and Rao 2009) found that perceived resource availability was a significant predictor of security policy compliance. Translated to university contexts, this finding suggests that investments in technical infrastructure and student-facing IT support services may yield returns not only in terms of reduced incident frequency but also in terms of enhanced student awareness and behavioral compliance.

The provision of endpoint security tools including antivirus software, virtual private networks (VPNs), and encrypted communication platforms through institutional channels has been identified as both a direct security measure and an indirect awareness-building mechanism. (Rhee, Kim et al. 2009) found that university students who used institutionally provided security tools demonstrated higher levels of cybersecurity awareness than those who relied on personal or free solutions, suggesting that the act of engaging with institutional security infrastructure may itself function as a form of practical security education.

2.5 Summary and Conclusion

This literature review has synthesized research across four key dimensions of cybersecurity awareness among university students: overall awareness levels, demographic influences, digital literacy and usage patterns, and institutional factors. The weight of evidence indicates that cybersecurity awareness among university students is generally inadequate, characterized by significant gaps between conceptual knowledge and behavioral practice, pronounced inequalities

across demographic groups, and considerable variation in the institutional environments that shape awareness outcomes.

Demographic research consistently identifies gender, academic discipline, and year of study as significant predictors of cybersecurity awareness, with male students, computing students, and more advanced students generally demonstrating higher technical knowledge. However, these effects are not universal and may be contingent on contextual and methodological factors. Research on digital literacy and usage patterns demonstrates that the quality and nature of digital engagement rather than simple exposure to technology is the more important predictor of cybersecurity awareness, with gamified learning, critical digital literacy education, and research-oriented internet use associated with higher awareness levels.

Institutional factors emerge as particularly powerful determinants of cybersecurity awareness, with well-designed awareness programs, clearly communicated and enforced policies, accessible IT support, and curriculum-integrated security education collectively contributing to higher levels of student awareness. The literature consistently points to the inadequacy of one-time, information-focused interventions and calls for comprehensive, sustained, and theoretically grounded approaches that address motivational and behavioral dimensions alongside knowledge.

In conclusion, improving cybersecurity awareness among university students requires a coordinated institutional response that recognizes the multidimensional nature of the problem and draws on the rich theoretical and empirical insights accumulated in the research literature. This review provides a comprehensive foundation for future empirical inquiry and practical intervention in this critical domain.

2.6 Limitations

Despite the growing body of research on cybersecurity awareness in higher education, several significant gaps remain. First, the literature is dominated by studies conducted in North American and Western European contexts, with relatively limited attention to cybersecurity awareness in developing country universities, particularly in Sub-Saharan Africa, South Asia, and Latin America(Chigada and Madzinga 2021);(Abubakar, Rasool et al. 2023). Given the distinct technological, economic, and institutional contexts of universities in these regions, there is a pressing need for empirically grounded, contextually sensitive research.

Second, the overwhelming majority of existing studies rely on cross-sectional survey designs, which preclude causal inference and limit understanding of how cybersecurity awareness develops over time. Longitudinal studies tracking students across their university careers would provide valuable insights into the developmental trajectories of cybersecurity awareness and the institutional factors that shape these trajectories ((Parsons, Crane et al. 2017); (Crossler, Johnston et al. 2013)

Third, while research has documented the awareness-behavior gap extensively, the psychological and contextual mechanisms that explain this gap remain insufficiently understood. Future research should draw more systematically on behavioral science frameworks including dual-process theories of decision-making, nudge theory, and situational action theory to develop more fine-grained accounts of the barriers to translating cybersecurity knowledge into secure behavior (Bada and Nurse 2019); (Sasse, Brostoff et al. 2001).

CHAPTER THREE: METHODOLOGY

3.0 Introduction

This chapter presents a detailed description of the research methodology that was employed to fulfil the four stated objectives of this study. The chapter outlines the research design, the study population, the sampling strategy and sample size determination the data collection procedures, data management practices and the data analysis techniques to be applied. Attention was given to the ethical considerations that guided the conduct of the study and to the limitations inherent in the chosen methodology.

3.1 Research Design

The study employed a cross-sectional survey research design. A cross-sectional design involved the collection of data from a representative sample of the study population at a single point in time, enabling the simultaneous examination of multiple variables and their interrelationships. This design was appropriate for the present study because it allowed for the efficient collection of data from a large and geographically concentrated population of university students, facilitates statistical comparison across demographic subgroups and enables the analysis of associations between the independent and dependent variables.

3.2 Study Population

The target population for this study comprised all currently enrolled undergraduate students at the study institution. Undergraduate students were selected as the unit of analysis because they constitute the most active digital users within the university environment, regularly engaging in

online academic research, social networking and digital communication. All activities that expose them to cybersecurity risks. The study further restricted the target population to students who had been enrolled for at least one complete semester as they had sufficient exposure to the institution's digital infrastructure and support systems to meaningfully respond to questions about institutional factors.

The accessible population were drawn from all academic colleges and schools within the institution ensuring broad representation across disciplines. This was important because cybersecurity awareness and digital literacy levels would vary across programs of study for instance, students in computing-related disciplines may possess higher baseline awareness compared to those in the humanities or social sciences. Inclusion of participants across all faculties therefore enhanced the representativeness of the study's findings.

3.3 Sampling Technique

The study employed a stratified random sampling technique. Stratified random sampling involves dividing the population into subgroups (strata) based on relevant characteristics and then randomly selecting respondents from within each stratum. The population is stratified according to academic colleges. Within each stratum, respondents were randomly selected to ensure that all the colleges were fairly represented in the study. This technique was selected over simple random sampling because it ensured that the sample adequately represents key subgroups relevant to the study's objectives, particularly academic college.

3.3.1 Sample size determination

The minimum required sample size for the study was determined using Yamane formulae for estimating a proportion in a large population since the population was known. For Makerere university, the estimated population of students was 38000.

Formula;

$$n = \frac{N}{1+N(e2)}$$

Were

- n = sample size
- N = Population size (38,000 students)
- e = acceptable margin of error (commonly 0.05 for 95% confidence level)

Substituting the values:

$n = 38000/ (1+38000(0.05^2))$

n = 38000/ (1+38000(0.0025))

n = 38000/ (1+95)

n = 38000/96

n = 395.83

Therefore, a minimum sample size of ~ 396 students were targeted.

3.4 Data Collection Procedure

The primary data collection instrument for this study was a structured questionnaire. The questionnaire was developed based on a comprehensive review of validated instruments used in prior cybersecurity awareness research. Items were adapted and contextualized to reflect the specific institutional and technological environment of Makerere University and the broader Ugandan higher education context.

The questionnaire was administered in digital formats to maximize response rates. The digital version was developed using Google Forms and distributed to students via their email accounts and social media platforms (WhatsApp). This approach helped ensure that responses were captured immediately and accurately. It also helped to reduce data entry errors because responses were automatically stored in a digital format. The responses were saved in a google account and later exported to Microsoft excel and SPSS for analysis.

3.5 DATA MANAGEMENT

This part of the chapter provided how data collected would be managed which includes data coding, data cleaning and handling of missing data.

3.5.1 Data coding

Categorical variables were coded numerically for example, gender was coded as 1 = Male, 2 = Female and year of study was coded as 1 = Year 1, 2 = Year 2, 3 = Year 3, and 4 = Year 4 and above

For the Likert-scale sections, responses were entered as numeric values (1–5) corresponding to the response categories. Composite scores for each construct digital literacy, institutional factor and

cybersecurity awareness were computed by summing or averaging the relevant items after verifying internal consistency.

3.5.2 Data Cleaning

Before analysis, the dataset was thoroughly cleaned to ensure accuracy and completeness. This involved;

Verification of data entry, where a random sample of entered, questionnaires was cross-checked to detect and correct any data entry errors.

Range checks, where all variables were checked to confirm that values fall within the expected range.

Consistency checks, that's to say logical inconsistencies were identified and resolved. For instance, a respondent recorded as a Year 1 student but who reports four years of prior university attendance will be flagged for review.

Duplicate record identification, where the dataset was screened for duplicate entries using unique identifiers, and confirmed duplicates were removed.

3.5.3 Handling Missing Data

Missing data would arise due to skipped questions or incomplete responses. The following approaches were used:

Assessment of Missing Data. The extent and pattern of missing data was examined (e.g., missing completely at random, missing at random). Questionnaires with a large proportion of missing responses were excluded from the analysis.

Non-response Treatment. For questionnaires with few missing values, appropriate methods were applied such as mean substitution for Likert-scale items within the same variable or pairwise deletion during statistical analysis to retain as many observations as possible.

Consistency Check After Imputation. After handling missing values, the dataset was rechecked to ensure no distortion of variable distributions.

3.6 DATA ANALYSIS

This was where conclusions were drawn from and it included preliminary analysis such as descriptive statistics and reliability analysis for the Likert-scale sections.

3.6.1 Preliminary Analysis

Prior to hypothesis testing, preliminary analysis was conducted to describe the sample and verify that the assumptions of the intended statistical tests were satisfied. Descriptive statistics including frequencies, percentages, means and standard deviations were computed for all study variables and reported in tabular form. The distribution of the dependent variable was examined for normality using the Shapiro-Wilk test and visually inspected using histograms. Reliability Analysis was conducted on the Likert-scale sections to confirm the factor structure of each construct before composite scores were formed.

3.6.2 Fitting Statistical Models and Selecting the Appropriate Model

The selection of the appropriate statistical model for each objective was guided by the following criteria: univariate analysis for each variable, bivariate analysis and multivariate analysis only for

the significant variables under the bivariate analysis. The table below summaries the planned analysis for each objective.

Table 3.1: Data Analysis plan by Objective

Objective	**Univariate analysis**	**Statistical Test**	**Assumptions checked**
Influence of age and gender on cybersecurity awareness	Descriptive statistics	Chi-square tests for age and gender	Pearson Chi-square (Asymptotic significance
Relationship between year of study and cybersecurity awareness	Descriptive statistics	Chi-square tests for age and gender	Pearson Chi-square (Asymptotic significance
Effect of digital literacy and digital usage patterns on cybersecurity awareness	Descriptive statistics	Chi-square tests for age and gender	Pearson Chi-square (Asymptotic significance

Influence of institutional factors on cybersecurity awareness	Descriptive statistics	Chi-square tests for age and gender	Pearson Chi-square (Asymptotic significance

3.7 ETHICAL CONSIDERATIONS

The conduct of this study followed strictly the ethical principles governing research involving human participants. Ethical clearance was sought from the Makerere University School of Statistics and Planning before any data collection activity commenced and no fieldwork begun until written approval was granted

Participation in the study was entirely voluntary. No form of coercion, inducement or academic incentive was used to encourage participation. Respondents were explicitly informed that their decision to participate or decline had no bearing on their academic standing, course grades or relationship with the university or any member of staff

The questionnaire did not collect any personal information such as names, student registration numbers or contact details. Respondents were assigned anonymous identification codes during data entry. All raw data were stored securely on a password-protected computer accessible only to the principal researcher.

Ethical clearance for the study was sought and obtained from the Makerere University School of Statistics and Planning prior to the commencement of data collection.

3.8 LIMITATIONS

Despite the care taken in designing this study, several methodological limitations were anticipated. These were acknowledged upfront in the spirit of transparency and mitigation strategies had been incorporated where feasible.

The cross-sectional survey design captured data at a single point in time making it impossible to draw definitive causal conclusions about the relationships between the independent variables and cybersecurity awareness. For example, while a significant association may be found between year of study and awareness, the design will not permit the conclusion that advancing through university causes awareness to increase. To mitigate this limitation, findings will be framed in relational rather than causal terms, and the researcher will recommend longitudinal designs for future research.

Second, the use of self-reported data introduces the possibility of social desirability bias, whereby respondents may overestimate their cybersecurity awareness or underreport risky behaviors to present themselves favorably. This limitation is mitigated to some extent by the assurance of anonymity provided to all respondents and by the inclusion of specific behavioral items that are less susceptible to social desirability effects than abstract attitudinal items.

The study will be conducted at a single institution, and the findings may not be directly generalizable to students at other universities with different digital infrastructure, academic cultures or student demographics. To enhance the transferability of findings, the researcher will provide a rich description of the study context and setting, enabling readers to make their own judgements about applicability to other contexts.

CHAPTER FOUR: RESULTS AND INTERPRETATION.

4.0 Introduction.

This chapter presents the results of the statistical analyses conducted to address the objectives of the study. This chapter begins with a test of normality and a reliability analysis to establish the suitability of the data for the planned statistical procedures. This is followed by univariate and bivariate analyses and finally a multivariate regression analysis that simultaneously examines the combined effect of the variables found to be significant at the bivariate level.

4.1 Normality test of the dependent variable.

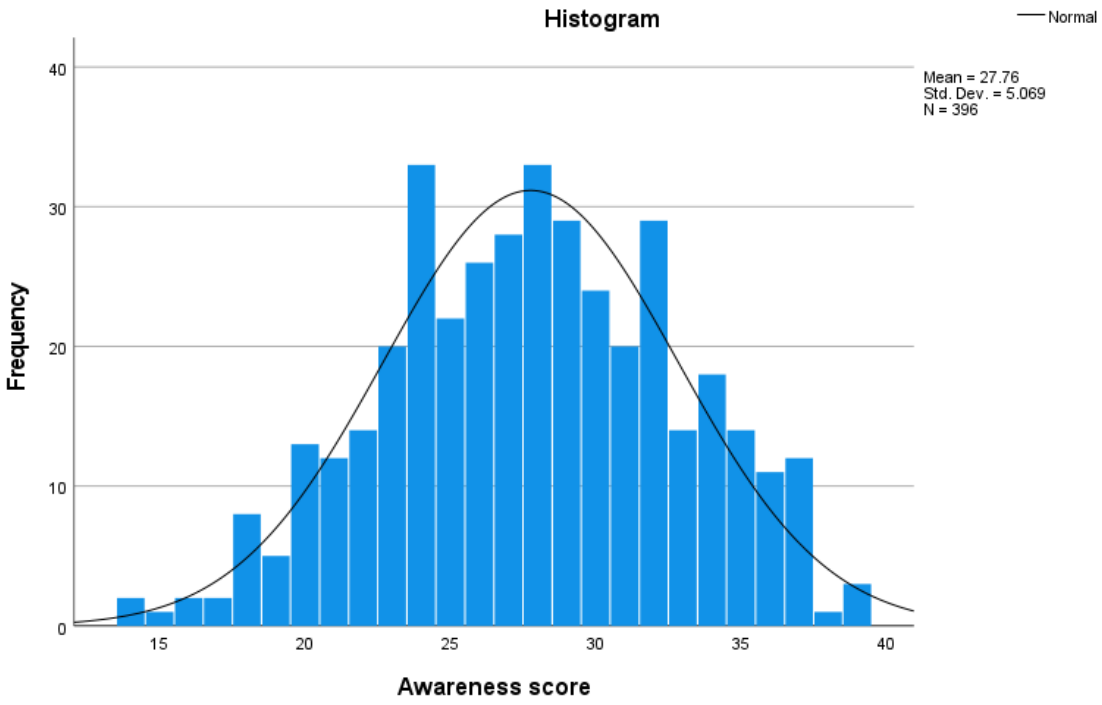


Figure 4.1 Normality test of dependent variable

Table 4.1 Tests for normality

	Statistics	df	Sig
Kolmogorov-Smirnov	0.056	396	0.005
Shapiro-Wilk	0.990	396	0.007

As shown in Table 4.1 and Figure 4.1, both tests returned statistically significant results (Kolmogorov-Smirnov statistic = 0.056, df = 396, p = 0.005; Shapiro-Wilk statistic = 0.990, df = 396, p = 0.007) indicated that the distribution of awareness scores departs significantly from a normal distribution, since both significance values fall below the conventional 0.05 threshold.

4.2 Reliability Analysis

Before conducting substantive analyses, the internal consistency of each Likert scale was assessed using Cronbach's alpha (α) coefficient. The results of the reliability analysis are presented below.

Table 4.2 Reliability analysis using Cronbach's alpha (α)

Construct	Cronbach's alpha (α)	Number of items
Awareness	0.735	8
Digital Usage	0.766	5
Digital Literacy	0.756	5
Institutional Support	0.796	6

All four scales demonstrate acceptable internal consistency ($\alpha > 0.70$). Institutional Support records the highest reliability ($\alpha = 0.796$), while Awareness shows the lowest but still acceptable reliability ($\alpha = 0.735$). These results confirmed that each composite score was a reliable measure of its intended construct, supporting the validity of subsequent analyses.

4.3 Univariate and bivariate analysis

4.3.1 The influence of demographic factors (age and gender) on cybersecurity awareness among students.

This sub-section examines whether student's demographic characteristics, specifically age and gender are associated with their level of cybersecurity awareness.

Descriptives statistics

Age group

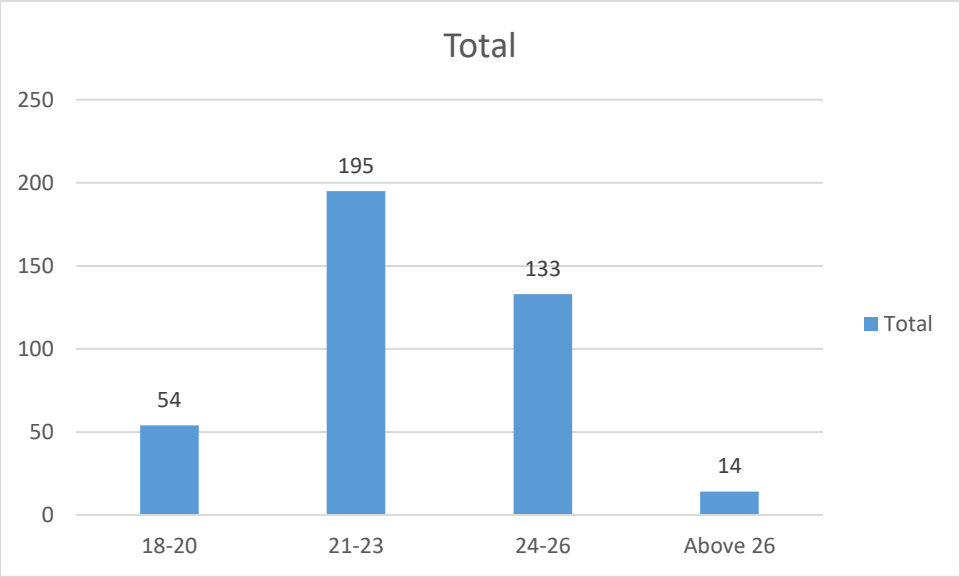


Figure 4.2 Age group distribution

The 21-23year age group recorded the highest number of respondents with 195 followed by 24-26year age group with 133, 18-20year age group with 54 and the lowest was recorded under the 26 and above age group with 14.

Gender.

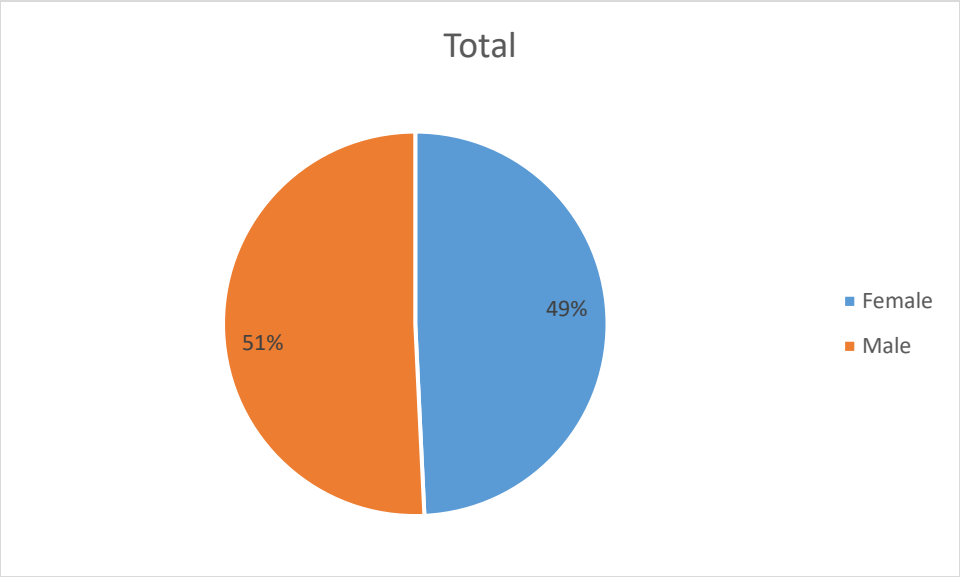


Figure 4.3 Gender distribution

The males responded highly with 51% and females with 49%.

Bivariate analysis.

Table 4.3: Chi-Square test for Age group and Gender.

Variables	**df**	**Pearson Chi-Square (Asymptotic significance(2-sided))**
Age group	84	0.134
Gender	28	0.358

The Pearson Chi-Square test revealed no statistically significant association between age and cybersecurity awareness (df = 84, p = 0.134) or between gender and cybersecurity awareness (df = 28, p = 0.358), since both significance values exceed the 0.05 threshold.

4.3.2 The relationship between year of study and cybersecurity awareness among students.

This sub-section examined whether student's year of study as an indicator of their level of academic progression was associated with their cybersecurity awareness.

Descriptives statistics

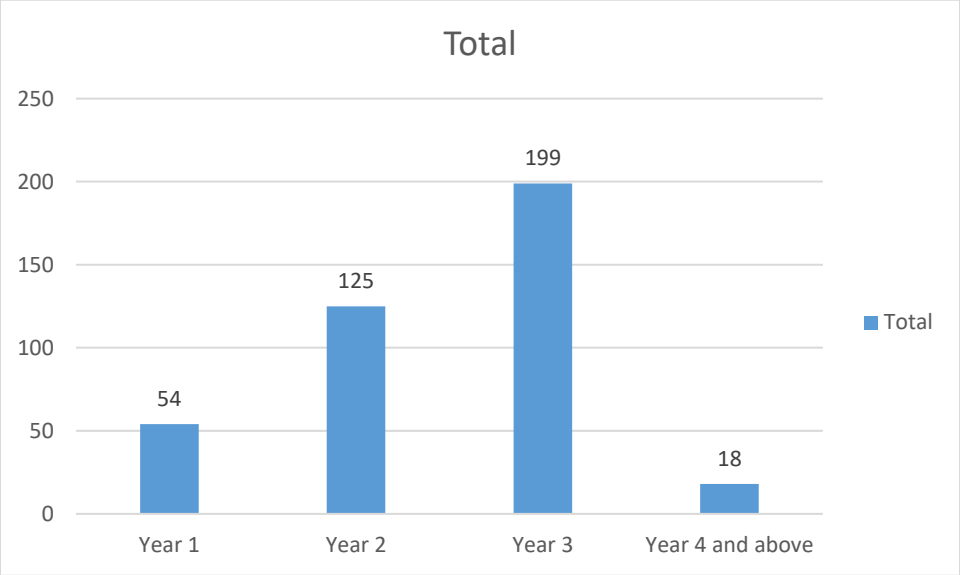


Figure 4.4 Student's Year of study

Year 3 students were the highest respondents with 199, followed by Year 2 students with 125, Year 1 students with 54 and Year 4 and above with 18.

Bivariate analysis

Table 4.4: Chi-Square test for Year of Study

Variable	df	Pearson Chi-Square (Asymptotic significance(2-sided))
Year of study	84	<0.001

Year of study was found to be significantly associated with cybersecurity awareness ($df = 75$, $p < 0.001$). The strength of this association was sufficient to meet the criterion ($p < 0.05$) for inclusion in the multivariate regression model.

4.3.3 The effect of digital literacy and digital usage patterns on cybersecurity awareness among students.

This sub-section examined the extent to which student's digital literacy and their patterns of digital usage were associated with their cybersecurity awareness.

Descriptives statistics

Table 4.5: Summary Statistics for Digital Literacy and Digital Usage.

Variable	Mean	Standard Deviation	Min	Max	Skewness
Digital Literacy	18.232	3.702	7	25	0.234
Digital Usage	19.520	3.641	9	25	0.301

The descriptive statistics for the digital literacy and digital usage composite scores. Respondents recorded a mean digital literacy score of 18.232 (SD = 3.702, range = 7–25) and a mean digital usage score of 19.520 (SD = 3.641, range = 9–25), placing both constructs moderately above the scale midpoint. Both distributions exhibited slight positive skewness (digital literacy skewness = 0.234; digital usage skewness = 0.301), well within the generally accepted range of ±1 for approximately symmetric distributions.

Usage patterns

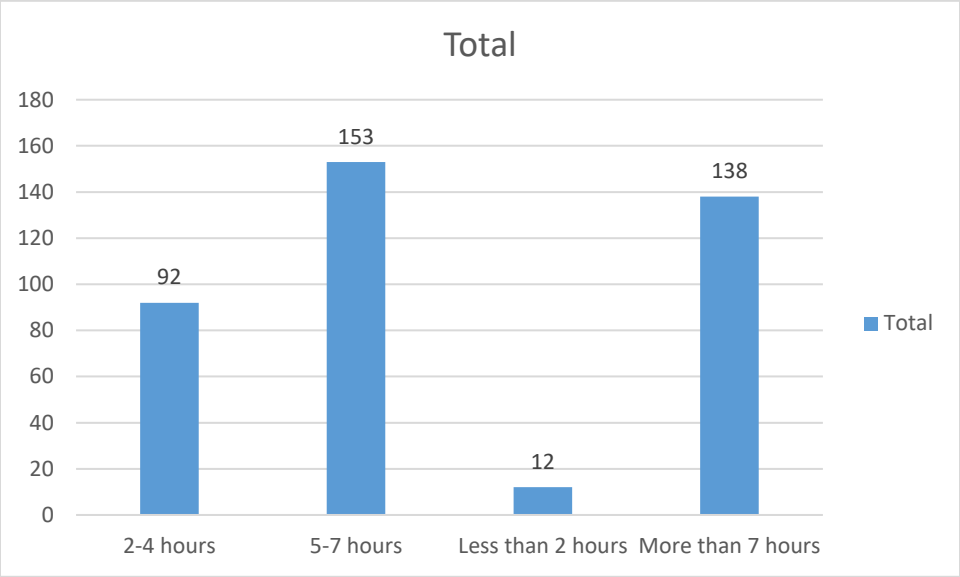


Figure 4.5 Usage patterns by hours

Under 5-7 hours, 153 students were recorded who conduct online activities followed by more than 7 hours with 138 students, 2-4 hours with 92 students and less than 2 hours with 12 students.

Bivariate analysis

Table 4.6: Chi-Square test for Digital Literacy and Digital Usage.

Variables	df	Pearson Chi-Square (Asymptotic significance(2-sided))
Digital Literacy	476	<0.001
Digital Usage	532	<0.001

Both digital literacy ($df = 476$, $p < 0.001$) and digital usage ($df = 532$, $p < 0.001$) were significantly associated with cybersecurity awareness.

4.3.4 The influence of institutional factors (availability of awareness programs and IT support systems) on cybersecurity awareness among students

This sub-section examined whether institutional factors were associated with student's cybersecurity awareness.

Descriptives statistics

Table 4.7: Summary Statistics for Institutional factors

Variable	Mean	Standard Deviation	Min	Max	Skewness
Institutional factors	16.846	4.601	6	30	0.198

The descriptive statistics for the institutional factors composite score recorded a mean of 16.846, standard deviation of 4.601 across a possible range of 6 to 30 and a low positive skewness value (0.198).

Bivariate analysis

Table 4.8: Chi-Square test for Institutional factors.

Variable	**df**	**Pearson Chi-Square (Asymptotic significance(2-sided))**
Institutional factors	644	<0.001

Institutional factors were significantly associated with cybersecurity awareness ($df = 644$, $p < 0.001$). This finding suggested that students who reported greater availability of institutional awareness programs and IT support systems also reported higher levels of cybersecurity awareness.

4.4 Multivariate analysis of all significant variables

Following the bivariate analyses presented in Section 4.3, year of study, digital literacy, digital usage and institutional factors were each found to be significantly associated with cybersecurity awareness ($p < 0.05$) and were therefore entered together into a multiple linear regression model to examine their combined and independent effects on cybersecurity awareness while controlling for one another.

Model summary

Table 4.9: Model Summary

Model	R	R Square	Adjusted R square
	0.575	0.331	0.324

The model summary presented in Table 4.9 indicates a multiple correlation coefficient of R = 0.575 suggested a moderate overall relationship between the combined predictor variables and cybersecurity awareness. The model accounted for $R^2 = 0.331$ of the variances in cybersecurity awareness with an adjusted R^2 of 0.324.

Analysis of Variance (ANOVA)

Table 4.10: Analysis of Variance

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	52.398	4	13.099	48.315	<0.001
Residual	106.010	391	0.271		
Total	158.408	395			

The analysis of variance presented in Table 4.10 confirms that the regression model as a whole is statistically significant, $F(4, 391) = 48.315$, $p < 0.001$. This indicated that the combination of year of study, digital literacy, digital usage and institutional factors significantly predicts cybersecurity awareness.

Regression Coefficients

Table 4.11: Regression Coefficients

Model	**Unstandardized coefficients B**	**Unstandardized coefficients St. Error**	**Standardized coefficients Beta**	**t**	**Sig**
(Constant)	1.150	0.199		5.785	<0.001
Year of Study	0.016	0.034	0.19	0.461	0.612
Literacy score	0.366	0.043	0.427	8.591	<0.001
Usage score	0.146	0.043	0.167	3.409	<0.001
Institutional score	0.135	0.036	0.164	3.791	<0.001

Table 4.11 present the unstandardized and standardized regression coefficients for each predictor in the model. Digital literacy emerged as the strongest predictor of cybersecurity awareness ($B = 0.366$, $\beta = 0.427$, $t = 8.591$, $p < 0.001$), followed by digital usage ($B = 0.146$, $\beta = 0.167$, $t = 3.409$, $p < 0.001$) and institutional factors ($B = 0.135$, $\beta = 0.164$, $t = 3.791$, $p < 0.001$) all of which were statistically significant predictors. By contrast, year of study did not retain statistical significance in the multivariate model ($B = 0.016$, $\beta = 0.19$, $t = 0.461$, $p = 0.612$).

CHAPETR FIVE: DISCUSSION, SUMMARY, CONCLUSION, RECOMMENDATION OF THE STUDY FINDINGS AND AREAS FOR FURTHER RESEARCH.

5.0 Introduction

This chapter discusses the findings presented in Chapter Four, summary, conclusion, recommendation of the study findings and areas for further study. Consistent with the analytical approach adopted in Chapter Four, the summary, conclusion and recommendations that follow the discussion focus primarily on those variables that retained statistical significance at the multivariate level.

5.1 Discussion of the findings

5.1.1 The influence of demographic factors (age and gender) on cybersecurity awareness among students.

Age

The finding that age was not significantly associated with cybersecurity awareness among students at Makerere University ($p = 0.134$) departs from the pattern reported in much of the existing literature. Older university students demonstrated higher cybersecurity awareness than their younger counterparts, attributing this to greater accumulated experience with real-world security incidents Harlington and Parsons (2017) while Sommestad, Hallberg et al. (2014) conversely, found that younger students displayed higher awareness of emerging technology-specific threats such as mobile security and social media privacy risks. The absence of a significant age effect in the present study may reflect the relatively narrow and homogenous age range typically found within a university student population, which may restrict the variability needed to detect age-

related differences that are more readily observed in samples spanning a wider age range. It may also suggest that within the specific context of Makerere University, exposure to cybersecurity-related information is relatively evenly distributed across age cohorts rather than concentrated among either older or younger students as theorized in the literature.

Gender

Gender was not significantly associated with cybersecurity awareness in this study ($p = 0.358$), a finding that contrasts with Shillair, Cotten et al. (2015), who reported that male students scored higher on objective measures of cybersecurity knowledge and Bhattacharya, Verma et al. (2023), who found that male students outperformed female peers specifically on technical knowledge items, although not on awareness of social engineering threats, across universities in the Gulf region. The absence of a significant gender gap in the present study may indicate that the gendered socialization patterns theorized to underlie these differences are less pronounced within the Makerere University student population than in the predominantly North American, European and Gulf-region contexts in which much of the existing literature is situated.

5.1.2 The relationship between year of study and cybersecurity awareness among students.

At the bivariate level, year of study was significantly associated with cybersecurity awareness ($p < 0.001$), broadly consistent with the literature's general observation that more academically advanced students tend to demonstrate higher technical knowledge of cybersecurity matters. However, this relationship did not persist once digital literacy, digital usage and institutional factors were controlled for in the multivariate regression model ($\beta = 0.19$, $p = 0.612$). This suggests that the apparent influence of year of study on cybersecurity awareness operates indirectly, through the accumulation of digital literacy and digital usage experience as student's

progress through their academic careers rather than through any direct effect of academic seniority itself. This interpretation is consistent with the developmental perspective implicit in the literature, whereby exposure and experience, rather than the simple passage of time or progression through an academic program, are understood to be the more proximate drivers of cybersecurity awareness.

5.1.3 The effect of digital literacy and digital usage patterns on cybersecurity awareness among students.

Digital literacy

Consistent with theoretical expectations, digital literacy emerged as the strongest predictor of cybersecurity awareness in the multivariate model ($\beta = 0.427$, $p < 0.001$). As Calvani, Fini et al. (2012) theorized that digital literacy as a foundational prerequisite for cybersecurity awareness given the conceptual overlap between the two constructs and directly replicating the finding of Contieri, Anholon et al. (2022) who reported that digital literacy significantly predicted cybersecurity knowledge among Portuguese university students. The present finding extends this evidence to a Sub-Saharan African university context, suggesting that the relationship between digital literacy and cybersecurity awareness identified in European samples generalizes to the Ugandan higher education setting.

Digital Usage

Digital usage was also a significant, though comparatively smaller, predictor of cybersecurity awareness ($\beta = 0.167$, $p < 0.001$). This finding is broadly consistent with Workman (2007), who found that the nature of student's online activities rather than usage frequency alone,

predicted security awareness with research and information-oriented use associated with greater awareness than purely social or entertainment-oriented use. It also resonates with the caution raised by Hadlington (2017) and Mylonas, Kastania et al. (2013), both of whom found that greater digital engagement particularly on mobile devices, does not automatically translate into safer behavior and can in some circumstances, be associated with greater risk-taking. The positive association observed in the present study suggests that on balance, students who reported more extensive digital usage also reported higher awareness, though the comparatively modest effect size relative to digital literacy implies that the quality and nature of digital engagement, as emphasized by Workman (2007), may be at least as important as its sheer extent.

5.1.4 The influence of institutional factors (availability of awareness programs and IT support systems) on cybersecurity awareness among students.

Institutional factors emerged as a statistically significant predictor of cybersecurity awareness ($\beta = 0.164$, $p < 0.001$), affirming the central role attributed to institutional context in the literature. This finding is consistent with Bulgurcu, Cavusoglu et al. (2010), who found that awareness initiatives effectively communicating the rationale behind security policies were more effective than compliance-oriented mandates. It also aligns with Rhee, Kim et al. (2009), who found that students who engaged with institutionally provided security tools demonstrated higher awareness than those relying on personal solutions, suggesting that institutional engagement may itself function as a form of practical security education. This finding carries particular significance in light of Chigada and Madzinga (2021), who documented that university cybersecurity awareness programs in South Africa were frequently under-resourced and inconsistently implemented,

contributing to persistently low awareness levels, and who called for a systems-level approach integrating cybersecurity education into the broader curriculum.

5.2 Summary.

At the multivariate level, the study revealed that digital literacy, digital usage and institutional factors were significant independent predictors of cybersecurity awareness among students at Makerere University. Age and gender showed no significant association with cybersecurity awareness at either the bivariate or multivariate level and although year of study was significantly associated with awareness at the bivariate level, it did not retain a statistically significant independent effect once digital literacy, digital usage and institutional factors were accounted for, indicating that its influence operates indirectly through these more proximate predictors.

5.3 Conclusion.

This study set out to examine the factors influencing cybersecurity awareness among university students focusing on demographic factors, year of study, digital literacy, usage patterns and institutional factors. The findings demonstrate that within the Makerere University context, cybersecurity awareness is most strongly shaped by student's digital literacy, the extent of their digital usage and the institutional environment in which they study rather than by demographic characteristics or academic seniority per se. These findings lend empirical support to theoretical accounts such as the hierarchical model of awareness proposed by Alotaibi, Furnell et al. (2023), that position digital competence as a foundational driver of cybersecurity awareness while also

extending the institutional perspective articulated by Bulgurcu, Cavusoglu et al. (2010) and Chigada and Madzinga (2021) to a Ugandan university setting.

5.4 Recommendations.

Based on the significant predictors identified at the multivariate level, the following recommendations are proposed.

Given that digital literacy emerged as the strongest predictor of cybersecurity awareness, the university should integrate structured digital literacy components that explicitly address cybersecurity concepts into existing digital skills curricula and student orientation programs, rather than treating digital literacy and cybersecurity education as separate undertakings.

In view of the significant effect of digital usage, the university should encourage purposeful and research-oriented patterns of digital engagement among students for example through information literacy instruction embedded within coursework.

For the significant effect of institutional factors, the university should strengthen the availability and visibility of cybersecurity awareness programs and IT support services, ensuring that these are designed to communicate the rationale for security practices rather than functioning as compliance mandates alone. It should also consider integrating cybersecurity education into the broader curriculum on a systems-level basis rather than relying on standalone or one-off interventions.

5.5 Area for further research.

Future research should therefore adopt longitudinal designs that track students over time to better understand the developmental trajectory of cybersecurity awareness.

This study examined statistical association between predictors and awareness but did not investigate the psychological and behavioral mechanisms underlying these relationships, nor the extent to which awareness translates into actual protective behavior. Future research should draw on behavioral science frameworks, including dual-process theories of decision-making, nudge theory and situational action theory, to better understand the awareness-behavior gap among students at Makerere University and similar institutions.

This study examined demographic, digital and institutional factors largely as independent predictors within a single regression model. Future research employing more sophisticated analytical techniques, such as structural equation modelling or multilevel analysis, could usefully examine whether these factors interact with one another, for example whether the effect of institutional support on cybersecurity awareness is conditional on students' baseline level of digital literacy.

REFERENCES

Abubakar, M., et al. (2023). "Comparative roles of IL-1, IL-6, IL-10, IL-17, IL-18, 1L-22, IL-33, and IL-37 in various cardiovascular diseases with potential insights for targeted immunotherapy." Cureus **15**(7).

Adams, A., et al. (2019). "The Report of the 2019 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure."

Afzal, M., et al. (2025). "How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario?" Journal of Cyber Security Technology **9**(2): 88-126.

Al-Janabi, S. and I. Al-Shourbaji (2016). "A study of cyber security awareness in educational environment in the middle east." Journal of Information & Knowledge Management **15**(01): 1650007.

Alenezi, M., et al. (2023). "The need of integrating digital education in higher education: Challenges and opportunities." Sustainability **15**(6): 4782.

Alotaibi, S., et al. (2023). Towards a framework for the personalization of cybersecurity awareness. International Symposium on Human Aspects of Information Security and Assurance, Springer.

Alqahtani, M. A. (2022). "Factors affecting cybersecurity awareness among university students." Applied Sciences **12**(5): 2589.

Bada, M. and J. R. Nurse (2019). "Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)." Information & Computer Security **27**(3): 393-410.

Ben-Asher, N. and C. Gonzalez (2015). "Effects of cyber security knowledge on attack detection." Computers in Human Behavior **48**: 51-61.

Bhattacharya, P., et al. (2023). "Game-o-meta: Trusted federated learning scheme for p2p gaming metaverse beyond 5g networks." Sensors **23**(9): 4201.

Bulgurcu, B., et al. (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security Awareness1." MIS quarterly **34**(3): 523-548.

Calvani, A., et al. (2012). "Are young generations in secondary school digitally competent? A study on Italian teenagers." Computers & Education **58**(2): 797-807.

Catal, C., et al. (2023). "Analysis of cyber security knowledge gaps based on cyber security body of knowledge." Education and Information Technologies **28**(2): 1809-1831.

Chigada, J. and R. Madzinga (2021). "Cyberattacks and threats during COVID-19: A systematic literature review." South African Journal of Information Management **23**(1): 1-11.

Contieri, P. G. S., et al. (2022). "Industry 4.0 enabling technologies in manufacturing: implementation priorities and difficulties in an emerging country." Technology Analysis & Strategic Management **34**(5): 489-503.

Crossler, R. E., et al. (2013). "Future directions for behavioral information security research." Computers & Security **32**: 90-101.

Elrayah, M. and S. Jamil (2023). "Impact of digital literacy and online privacy concerns on cybersecurity behaviour: The moderating role of cybersecurity awareness." International Journal of Cyber Criminology **17**(2): 166-187.

Gwenhure, A. K. (2025). "University students' security behavior against email phishing attacks: insights from the health belief model." Journal of Cybersecurity **11**(1): tyaf034.

Hadlington, L. (2017). "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours." Heliyon **3**(7).

Hadlington, L. and K. Parsons (2017). "Can cyberloafing and internet addiction affect organizational information security?" Cyberpsychology, Behavior, and Social Networking **20**(9): 567-571.

Herath, T. and H. R. Rao (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." European Journal of information systems **18**(2): 106-125.

Mphatheni, M. R. and W. Maluleke (2022). "Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions." International journal of research in business and social science **11**(4): 384-396.

Mylonas, A., et al. (2013). "Delegate the smartphone user? Security awareness in smartphone platforms." Computers & Security **34**: 47-66.

Ng, B.-Y., et al. (2009). "Studying users' computer security behavior: A health belief perspective." Decision Support Systems **46**(4): 815-825.

Niyikora, E. (2025). Cybersecurity Risk Assessment Methods for Digital Financial Services in Sub-Saharan Africa, Walden University.

Nyasvisvo, B. and J. M. Chigada (2023). "Phishing attacks: a security challenge for university students studying remotely." The African Journal of Information Systems **15**(2): 3.

Oroni, C. Z., et al. (2025). "Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students." Education and Information Technologies **30**(10): 14197-14236.

Parsons, C. E., et al. (2017). "Home practice in mindfulness-based cognitive therapy and mindfulness-based stress reduction: a systematic review and meta-analysis of participants' mindfulness practice and its association with outcomes." Behaviour research and therapy **95**: 29-41.

Rhee, H.-S., et al. (2009). "Self-efficacy in information security: Its influence on end users' information security practice behavior." Computers & Security **28**(8): 816-826.

Sasse, M. A., et al. (2001). "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security." BT technology journal **19**(3): 122-131.

Shillair, R., et al. (2015). "Online safety begins with you and me: Convincing Internet users to protect themselves." Computers in Human Behavior **48**: 199-207.

Sommestad, T., et al. (2014). "Variables influencing information security policy compliance: A systematic review of quantitative studies." Information Management & Computer Security **22**(1): 42-75.

Tasnim, M., et al. (2025). Determining cybersecurity awareness and human-cyber behaviour in Bangladeshi women: Addressing factors, risks and overcoming knowledge disparities, BRAC University.

Tsai, H.-y. S., et al. (2016). "Understanding online safety behaviors: A protection motivation theory perspective." Computers & Security **59**: 138-150.

Workman, M. (2007). "Gaining access with social engineering: An empirical study of the threat." Information Systems Security **16**(6): 315-331.

APPENDIX

QUESTIONNAIRE: CYBERSECURITY AWARENESS AMONG UNIVERSITY STUDENTS

Section A: Demographic Information

1. Age:

   ☐ 18–20

   ☐ 21–23

   ☐ 24–26

   ☐ Above 26

2. Gender:

   ☐ Male

   ☐ Female

3. Year of Study:

   ☐ Year 1

   ☐ Year 2

   ☐ Year 3

   ☐ Year 4 and above

4. Field of study

   CAES

   COBAMS

   COCIS

   CEES

   CEDAT

   CHS

   CHUSS

   CONAS

   COVAB

Section B: Cybersecurity Awareness

Instruction: Indicate your level of agreement with the following statements:
1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree

1. I understand what cybersecurity means.
2. I can identify phishing emails or messages.
3. I regularly update my passwords.

4. I use strong and unique passwords for different accounts.
5. I am aware of common cyber threats (e.g., malware, hacking).
6. I avoid clicking suspicious links.
7. I know how to protect my personal information online.
8. I use antivirus or security software on my devices.
9. I understand the risks of using public Wi-Fi.

Section C: Digital Literacy

Likert Scale (1–5 as above)

1. I am confident using computers and mobile devices.
2. I can install and update software on my devices.
3. I understand privacy settings on social media platforms.
4. I can recognize unsafe websites.
5. I know how to secure my online accounts.
6. I can troubleshoot basic technical issues.

Section D: Digital Usage Patterns

1. How many hours do you spend online daily?

   ☐ Less than 2 hours

   ☐ 2–4 hours

   ☐ 5–7 hours

   ☐ More than 7 hours

Likert Scale (1–5):

2. I frequently use social media platforms.

3. I conduct academic activities online.
4. I use public Wi-Fi networks.
5. I download files or software from the internet.
6. I perform online transactions (e.g., mobile money, banking).

Section E: Institutional Factors

Likert Scale (1–5):

1. My university provides cybersecurity awareness programs.
2. I have attended cybersecurity training or workshops.
3. The university provides adequate IT support services.
4. I receive guidance on safe internet practices from the university.
5. The university communicates cybersecurity risks effectively.
6. IT systems at the university are secure and reliable.

Section F: Additional Insight

1. Have you ever experienced a cybersecurity incident?

   ☐ Yes

   ☐ No

2. If yes, briefly describe:

3. What do you think can improve cybersecurity awareness among students?