THE ROLE OF SOCIAL ENGINEERING IN CAMPUS-BASED CYBERCRIMES

BY

EMMANUEL OSAMUYI OTA

PSC2105401

DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF PHYSICAL SCIENCES,

UNIVERSITY OF BENIN,

BENIN CITY,

EDO STATE, NIGERIA.

NOVEMBER 2025

THE ROLE OF SOCIAL ENGINEERING IN CAMPUS-BASED CYBERCRIMES

BY

EMMANUEL OSAMUYI OTA

PSC2105401

A PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF PHYSICAL SCIENCES, UNIVERSITY OF BENIN, BENIN CITY

IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF A BACHELOR OF SCIENCE (B.Sc.) DEGREE IN COMPUTER SCIENCE

NOVEMBER 2025

CERTIFICATION

This is to certify that this project work was carried out by **EMMANUEL OSAMUYI OTA** with Matriculation Number **PSC2105401** under my supervision. It is adequate and satisfactory, both in scope and content, for the award of Bachelor of Science (B.sc) Degree in Computer Science of the University of Benin

---

PROF. (MRS.) S. KONYEHA
Project Supervisor

DATE

APPROVAL

This project work is hereby approved in partial fulfilment of the requirements for the award of Bachelor of Science (B.Sc.) Degree in Computer Science from the University of Benin.

DR. ROSEMARY USIOBAIFO
Head of Department

DATE

DEDICATION

This project is dedicated to God Almighty for giving me the strength and wisdom to see it through to completion, and even throughout my stay in the University of Benin (UNIBEN). It is also dedicated to my best friend the holy spirit for the strength and the grace to function effectively in this course of mine and also to my parents who were there for me in the most supportive way a parent could be and for their love, support and guidance throughout my academic journey.

ACKNOWLEDGEMENT

My utmost acknowledgement goes to God Almighty for giving me the strength, wisdom and direction throughout my academic journey. I would like to express my gratitude to my project supervisor, Prof. (Mrs.) S. KONYEHA for her consistent guidance towards ensuring the successful completion of this project.

I would also like to specially thank my highly esteemed Head of Department of Computer Science Dr. Rosemary Usiobaifo for her outstanding leadership and my project coordinator Dr. Maxwell Osagie, and other lecturers in the Department of Computer Science who I have been opportune to cross paths with, and have impacted me immensely these past few years: Prof. G.O. Ekuobase, Dr. F.O. Oliha, Prof. A.A. Imiavan, Prof. (Mrs.) F. Egbokhare, Prof. (Mrs.) V.V.N. Akwukwuma, Prof. F.I. Amadin, Prof. (Mrs.) V.I. Osubor, Dr. (Mrs.) Aziken, Prof. F.O. Chete, Dr. (Mrs) R.O. Osaseri, Mr. P. E.B. Imiefoh, Mr. I.E. Obasohan, Mr. K.O. Otokiti, Mr. I.E. Obayagbonna, Mrs. R.I. Izevbizua, Dr. E.C. Igodan, and Miss L. O. Usiosefe, Finally, I also want to appreciate my parents Apostle and Rev. Mrs. Ota who contributed to the success of this project. I would also like to thank my siblings: Samuel, Abigail, and Vera for their love and care, and my friends for their support, words of encouragement, and consistent guidance throughout this project. Finally to Chosen Family, thank you all for being the best family in the world.

TABLE OF CONTENTS

CERTIFICATION ii

APPROVAL iii

DEDICATION iv

ACKNOWLEDGEMENT v

TABLE OF CONTENTS vi

LIST OF TABLES xii

LIST OF FIGURES xiii

ABSTRACT xiv

CHAPTER ONE 1

INTRODUCTION 1

1.1 Background to the Study 1

1.2 Statement of the Problem 2

1.3 Aim and Objectives of the Study 2

1.4 Significance of the Study 3

1.5 Research Questions 4

1.6 Scope of the Study 4

1.7 Limitations 4

1.8 Definition of Terms 5

CHAPTER TWO 6

LITERATURE REVIEW 6

2.1 Introduction 6

2.2 Conceptual Clarifications 6

2.2.1 Definition of Social Engineering 6

2.2.2 Types of Social Engineering 7

2.2.3 Psychological Elements and Vulnerability 7

2.2.4 Digital Literacy and Awareness Gaps 8

2.3 Cybercrime in Campus Environments 8

2.3.1 Nature of Campus-Based Cybercrime 8

2.3.2 Student-Specific Vulnerabilities 8

2.3.3 Institutional Weaknesses and Campus Culture 8

2.4 Theoretical Frameworks 9

2.4.1 Human Hacking Model (Hadnagy, 2021) 9

2.4.2 Routine Activity Theory (Cohen & Felson, 2020) 9

2.4.3 Deception Theory (Burgoon, 2020) 9

2.5 Empirical Evidence from Nigeria and Beyond 9

2.5.1 Frequency and Patterns 9

2.5.2 Awareness and Behavioral Analysis 10

2.5.3 Mitigation Case Studies 10

2.6 Mitigation and Awareness Strategies 10

2.6.1 Institutional Measures 10

2.6.2 Curriculum Integration and Cyber Hygiene Training 10

2.6.3 Peer and Community-Based Awareness 10

2.7 Research Gaps and Justification 11

2.8 Review of Related Empirical Studies 11

Discussion of Related Works 13

CHAPTER THREE 14

RESEARCH METHODOLOGY 14

3.0 Introduction 14

3.1 Research Design 14

3.2 Area of Study (Study Location) 16

3.3 Population of the Study 17

3.4 Sample Size and Sampling Technique 18

3.5 Research Instruments 20

3.5.1 Questionnaire 20

3.5.2 Interview Guide 21

3.5.3 Justification for Instruments Used 22

3.5.4 Existing System (Current Complaint Reporting Process) 22

3.6 Validity and Reliability of the Instruments 23

3.6.1 Validity of the Instruments 23

3.6.2 Reliability of the Instruments 24

3.7 Method of Data Collection 25

3.7.1 Administration of Questionnaires 25

3.7.2 Conduct of Interviews 26

3.7.3 Secondary Data Collection 26

3.8 Method of Data Analysis 27

3.8.1 Preparation of Data 27

3.8.2 Quantitative Data Analysis 28

3.8.3 Qualitative Data Analysis 30

3.8.4 Presentation of Results 31

3.8.5 Linking Analysis to Research Objectives 32

3.8.6 Software Tools 32

3.8.7 Limitations of the Analysis 32

3.9 Ethical Considerations 33

3.9.1 Ethical Approval 33

3.9.2 Informed Consent 33

3.9.3 Confidentiality and Anonymity 34

3.9.4 Data Protection 34

3.9.5 Avoidance of Harm 34

3.9.6 Academic Integrity and Objectivity 35

3.9.7 Ethical Conduct in Reporting 35

3.10 Summary 35

CHAPTER FOUR 37

DATA PRESENTATION, ANALYSIS, AND INTERPRETATION 37

4.0 Introduction 37

4.1 DATA PRESENTATION 38

4.1.1 Questionnaire Distribution and Retrieval 39

4.1.2 Demographic Characteristics of Respondents 39

4.2 Demographic Characteristics of Respondents 42

4.2.1 Gender Distribution 42

4.2.2 Age Distribution 43

4.2.3 Respondent Category 43

4.2.4 Faculty/Departmental Distribution 44

4.2.5 Level of ICT Exposure 45

4.3 Predominant Social Engineering Tactics Targeting Students 45

4.3.1 Behavioral and Environmental Factors Heightening Student Susceptibility 48

4.3.2 Tailored Intervention Strategies and Preventive Measures 50

4.4 System Prototype (Campus Cyber Complaint Portal) 53

4.5 Discussion of Findings 57

4.5.1 Interpretation of Quantitative Findings 57

4.5.2 Comparison with Previous Studies 58

4.5.3 Implications for Campus Cybersecurity Policies 59

4.6 Summary of Major Findings 59

4.7 Conclusion 60

CHAPTER FIVE 61

SUMMARY, CONCLUSION, AND RECOMMENDATIONS 61

5.1 Summary of the Study 61

5.2 Summary of Major Findings 62

5.3 Conclusion 63

5.4 Recommendations 63

5.5 Suggestions for Further Studies 65

5.6 Contribution to Knowledge 66

5.7 Concluding Remark 66

REFERENCES 67

APENDIX 69

LIST OF TABLES

Table 2.1: Summary of Related Empirical Studies

Table 4.1: Questionnaire Distribution and Retrieval

Table 4.2: Gender Distribution of Respondents

Table 4.3: Age Distribution of Respondents

Table 4.4: Category of Respondents

Table 4.5: Internet Usage Among Respondents

Table 4.6: Predominant Social Engineering Tactics Targeting Students

Table 4.7: Behavioral and Environmental Factors Contributing to Student Susceptibility

LIST OF FIGURES

Figure 4.1: Homepage of the Campus Cyber Complaint Portal

Figure 4.2: Online Complaint Submission Form Interface

Figure 4.3: Administrative Dashboard for Viewing and Managing Reports

ABSTRACT

This study examined the role of social engineering in campus-based cybercrimes, focusing on Nigerian tertiary institutions with the University of Benin as case study. Social engineering continues to thrive in academic environments due to trust-based communication systems and increasing reliance on digital platforms for academic, financial, and social interactions. A mixed-method research design was adopted, combining structured questionnaires administered to 400 respondents and semi-structured interviews with key ICT personnel. Findings revealed phishing, impersonation, and fake scholarship scams as the most prevalent social engineering tactics. Behavioral factors such as curiosity, peer influence, and financial vulnerability were identified as major contributors to student susceptibility, alongside institutional gaps including weak cyber awareness programs and poor reporting mechanisms. The study further established that although many students possess basic digital skills, deeper cybersecurity literacy remains insufficient. To address this, the research proposes targeted awareness interventions and the implementation of a Campus Cyber Complaint Reporting System to support early detection, incident reporting, and response coordination. The study concludes that proactive training and structured institutional response measures are essential in reducing the success of social engineering attacks within university environments.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Social engineering represents a major non-technical cyber threat that relies on psychological manipulation such as trust, urgency, authority, and peer influence to deceive individuals into divulging sensitive information or performing compromising actions (Okokpujie et al., 2025; Nwajioha & Oshim, 2025). Within Nigerian university environments, these attacks commonly appear through phishing emails, impersonated WhatsApp accounts, cloned social media identities, and deceptive scholarship or job offers targeted at students (Okokpujie et al., 2025).

A study conducted among Covenant University students revealed that more than 70% of respondents were susceptible to phishing simulations despite reporting high awareness of cyber risks, showing a critical gap between knowledge and behavior (Okokpujie et al., 2025). Similarly, research at Ebonyi State University emphasized the growing exposure of campus populations to identity fraud and online deception, recommending proactive campus-level intervention programs (Nwajioha & Oshim, 2025).

Although social engineering often results in financial loss, identity theft, academic disruption, and emotional trauma, many Nigerian tertiary institutions lack structured awareness frameworks and centralized reporting systems to address these human-centered threats (Aguiyi et al., 2025). Instead, existing cybersecurity measures remain heavily focused on technical controls such as passwords and firewalls, while the human element remains largely unprotected (Badamasi & Utulu, 2021).

This study therefore examines how social engineering techniques are deployed within university environments, why students remain vulnerable, and what targeted strategies including structured reporting mechanisms can effectively reduce the success of such attacks.

1.2 Statement of the Problem

The increasing dependence on digital platforms for academic communication, registration processes, and social interaction has widened the attack surface for social engineering in university environments. Students often receive fraudulent emails, impersonated messages, and manipulated communication that appear credible (Okokpujie et al., 2025).

However, despite frequent exposure to these attacks, most students lack the skills necessary to verify authenticity or identify deceptive patterns, leading to unintentional disclosure of login credentials, financial information, or personal details (Nwajioha & Oshim, 2025). Institutional responses remain reactive rather than preventive, with no centralized mechanism for reporting cyber incidents, meaning cases often go undocumented and unresolved (Aguiyi et al., 2025).

This gap leaves students vulnerable, institutions underprepared, and campus digital ecosystems exposed to repeated cycles of manipulation.

1.3 Aim and Objectives of the Study

The aim of this study is to investigate the role of social engineering in campus-based cybercrimes and to propose effective strategies to enhance student cybersecurity awareness and resilience in Nigerian universities.

Objectives of the Study

The specific objectives of the study are to:

1. Identify the predominant social engineering tactics used to target students within Nigerian academic environments.
2. Analyze the behavioral and environmental factors that heighten student vulnerability to social engineering attacks.
3. Propose tailored preventive and intervention strategies to minimize the success of these attacks, including the development of a Campus Cyber Complaint Reporting System to support timely incident reporting and response.

1.4 Significance of the Study

The study contributes to academic understanding by providing empirical insights into how psychological and social factors influence susceptibility to cyber manipulation. Practically, the findings will:

- Guide university ICT units in designing effective awareness and response programs.
- Equip students with knowledge to recognize and resist manipulative digital interactions.
- Support the development of a centralized Campus Cyber Complaint Portal for structured reporting, monitoring, and intervention.

The study aligns with national efforts to improve cyber hygiene, strengthen digital literacy, and promote safer learning environments across Nigerian tertiary institutions.

1.5 Research Questions

This study is guided by the following research questions:

1. What are the most common social engineering techniques deployed to exploit students in Nigerian universities?
2. Which behavioral and campus-based factors contribute to student vulnerability?

What targeted awareness and preventive strategies can effectively reduce the success of social engineering attacks?

1.6 Scope of the Study

This study focuses on social engineering-based cyber threats such as phishing, impersonation, baiting, and deceptive digital communication targeting students within Nigerian universities. The investigation draws on data collected from the University of Benin. Technical system-level hacking, malware attacks, and cryptographic exploitation are beyond the scope of this study.

1.7 Limitations

1. Absence of a Campus Cyber Complaint Portal for reporting cases of social engineering prevalence on campus
2. Results of analysis rely on self-reported data which may include recall or social desirability bias
3. Sample representativeness is limited to UNIBEN context; generalization to other universities should be cautious.

1.8 Definition of Terms

- Social Engineering: In very simple terms, social engineering is when someone tricks people into giving away information, access, or doing something they normally wouldn't do by using psychology instead of hacking computers.
- Cybercrime: It is any illegal activity that uses computers, networks, or the internet, such as stealing data, breaking into systems, or scamming people online.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

A robust literature review is essential to establish the theoretical and empirical foundation of this study. Social engineering is a highly adaptive cyber threat vector, and its impact within campus environments, particularly Nigerian universities, has received limited scholarly attention. This chapter synthesizes global and Nigerian studies to present a multidisciplinary understanding of social engineering, incorporating psychological, educational, technological, and criminological perspectives.

The review progresses from conceptual foundations and typologies to campus-specific vulnerabilities, institutional responses, and theoretical frameworks underpinning the study. The chapter concludes with research gaps that justify the need for the present study.

2.2 Conceptual Clarifications

2.2.1 Definition of Social Engineering

Social engineering refers to the strategic use of deception to manipulate individuals into revealing confidential information or performing unauthorized actions. According to Gragg (2020), social engineering exploits human behavior rather than technical vulnerabilities, often leveraging authority, urgency, and trust. Shahzad et al. (2022) affirmed that even in systems supported by technological security, individuals may still be compromised due to psychological manipulation.

Within Nigerian universities, cultural norms such as hierarchical respect and communal trust further contribute to vulnerability in student digital interactions.

2.2.2 Types of Social Engineering

Researchers classify social engineering into various forms, including:

Type of Attack	Academic Illustration
Phishing and Spear Phishing	Fraudulent emails impersonating school ICT units or scholarship boards (Olajide et al., 2021).
Pretexting	Fake identity or scenario used to deceive students (Uche & Adebayo, 2022).
Baiting and Drops	USB Malicious files or USB drives left in libraries or labs (Adeleke & Sanni, 2021).
Quid Pro Quo	Offering benefits in exchange for login details (Ogundele et al., 2023).
Social Network Deception	Attackers clone student or lecturer profiles on social media (Martins, 2023).

Students' heavy use of messaging platforms such as WhatsApp and Telegram further increases exposure.

2.2.3 Psychological Elements and Vulnerability

Social engineering exploits predictable psychological triggers such as curiosity, urgency, fear, and trust (Bada et al., 2022). IBM (2023) reported that human error contributes to nearly 95% of cybersecurity breaches. Cognitive biases such as authority bias, social proof, and scarcity effect also explain why students comply even when threats appear suspicious.

2.2.4 Digital Literacy and Awareness Gaps

Digital literacy refers to the ability to critically evaluate digital content and communications. Studies indicate that over 60% of Nigerian university students cannot reliably detect phishing attempts (Okafor & Adewale, 2023). UNESCO (2022) projected national digital literacy improvements but noted infrastructural gaps. Bello & Ajao (2024) highlighted that digital security is often missing from university curricula, creating structural vulnerability.

2.3 Cybercrime in Campus Environments

2.3.1 Nature of Campus-Based Cybercrime

Campus-based cybercrimes include phishing scams, academic fraud, credential harvesting, identity theft, and financial scams. Okoye & Alhassan (2022) explained that attackers exploit shared networks and informally trusted communication channels. Eze & Yusuf (2020) noted that weak password habits and reused login credentials remain critical risk points.

2.3.2 Student-Specific Vulnerabilities

Students frequently share devices and reuse passwords, enabling attacker success (Nwogu & Agbo, 2022). Vulnerability is influenced by factors such as faculty discipline, digital habits, and gender (Ugwu et al., 2023). Students also rely heavily on social groups and informal digital communication, increasing susceptibility to manipulation.

2.3.3 Institutional Weaknesses and Campus Culture

Many Nigerian universities lack structured campus-wide cyber hygiene frameworks. While Badamasi & Utulu (2021) proposed an institutional risk management framework,

implementation remains inconsistent. Public universities in particular often rely on reactive responses rather than preventive awareness programs.

2.4 Theoretical Frameworks

2.4.1 Human Hacking Model (Hadnagy, 2021)

This model explains social engineering attacks as a cycle: information gathering → rapport building → exploitation → exit. On campuses, attackers gather data from social media and class forums before launching impersonation or phishing attacks.

2.4.2 Routine Activity Theory (Cohen & Felson, 2020)

Cybercrime occurs when a motivated offender, a suitable target, and absence of digital guardianship converge. Nigerian campuses, with open networks and informal digital culture, fit these conditions.

2.4.3 Deception Theory (Burgoon, 2020)

Deception Theory explains how verbal and nonverbal cues are manipulated in communication. This aligns with impersonation attacks conducted through messaging platforms and fake institutional announcements.

2.5 Empirical Evidence from Nigeria and Beyond

2.5.1 Frequency and Patterns

Olajide et al. (2021) recorded widespread phishing in universities, while Martins (2023) established strong links between social media exposure and attack likelihood. Nwogu & Agbo (2022) noted that 37% of undergraduates have experienced a social engineering attempt.

2.5.2 Awareness and Behavioral Analysis

Ugwu et al. (2023) found that awareness varies based on gender and academic discipline. Okafor & Adewale (2023) confirmed awareness does not guarantee safe behavior, aligning with cognitive bias theory. Bamidele et al. (2021) explored psychological influences behind compliance.

2.5.3 Mitigation Case Studies

Ojugo & Otakore (2018) demonstrated that simulation-based awareness training reduces phishing success. National initiatives such as NITDA's Digital States and 3MTT Programs (2021–2024) aim to strengthen national cyber resilience.

2.6 Mitigation and Awareness Strategies

2.6.1 Institutional Measures

Universities implementing mandatory cyber awareness programs and ICT policies show reduced attack success (Badamasi & Utulu, 2021).

2.6.2 Curriculum Integration and Cyber Hygiene Training

Role-play phishing simulations and hands-on digital safety workshops are effective when incorporated into general studies and departmental training.

2.6.3 Peer and Community-Based Awareness

NACOS-led peer-to-peer cybersecurity clubs have shown better behavioral change than official circulars due to social influence patterns.

2.7 Research Gaps and Justification

Although global studies offer strong theoretical frameworks, Nigeria-specific empirical evidence remains limited. There is insufficient research on:

- How student digital habits influence susceptibility
- The role of campus peer-network influence
- The effectiveness of institutional reporting and response systems

This study addresses these gaps by examining behavioral, environmental, and institutional factors within a Nigerian campus and proposing a Campus Cyber Complaint Reporting System as a practical intervention.

2.8 Review of Related Empirical Studies

A number of empirical studies have examined social engineering and cybersecurity within academic environments, both locally and internationally. These studies provide comparative insights that strengthen the current research. Table 2.1 summarizes some key related works, highlighting their focus, methodology, and outcomes.

Table 2.1: Summary of Related Empirical Studies

Author(s) & Year	Study Focus	Methodology	Key Findings	Relevance to Present Study
Adebayo & Ogunleye (2021)	Phishing awareness among Nigerian undergraduates	Survey of 300 students	68% failed simulated phishing tests	Demonstrates high vulnerability within student populations
Chukwuma & Eze (2023)	Behavioral analysis of cyber deception in tertiary institutions	Mixed methods	Financial need and peer influence were top enablers	Supports behavioral dimension of this study
Ibrahim et al. (2023)	Patterns of campus-based cybercrime in Nigeria	Quantitative	41% of students reported impersonation-related scams	Reinforces prevalence within Nigerian universities
Olajide et al. (2021)	Phishing susceptibility among university users	Experimental study	Awareness did not significantly reduce vulnerability	Emphasizes the need for psychological-based interventions
Ugwu et al. (2023)	Gender and discipline in cybersecurity awareness	Quantitative	Female students exhibited higher caution levels	Useful for demographic comparison
Ojugo & Otakore (2018)	Effectiveness of cyber awareness campaigns	Quasi-experimental	Simulations improved detection by 47%	Basis for recommending institutional awareness programs
Afolabi & Iroko (2022)	Human factor analysis in university cyber breaches	Survey	74% of incidents linked to user error	Correlates with human-centered cyber threats in this research
Badamasi & Utulu (2021)	Risk management framework for Nigerian universities	Conceptual model	Framework proposed but weak implementation	Highlights institutional gap addressed by this study
Sheng et al. (2019)	Global phishing behavior study	Quantitative	Younger users most likely to click links	Validates focus on student demographics

Author(s) & Year	Study Focus	Methodology	Key Findings	Relevance to Present Study
Weir & Douglas (2021)	Human-based cyber risk	Case study	Training reduces incident frequency	Aligns with preventive strategy component of this work

Discussion of Related Works

The reviewed studies collectively underscore that social engineering remains a dominant cyber threat within university settings, primarily driven by low awareness, financial motives, and weak institutional frameworks. Most studies employed survey or experimental methods, revealing consistent trends of human error as a major vulnerability factor. However, while existing research emphasizes awareness and policy, few propose or implement practical reporting systems, especially in Nigerian contexts. This gap justifies the development of the Campus Cyber Complaint Portal proposed in this study as a sustainable institutional response.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter focuses on the methods and procedures adopted in carrying out the study. It outlines the framework through which data relevant to the research objectives were obtained, analyzed, and interpreted. Since this research seeks to examine the role of social engineering in campus-based cybercrimes, a well-defined methodology is essential to ensure that the findings are valid, reliable, and applicable within academic environments. The methodology provides a clear blueprint for how the research questions were addressed by identifying the research design, population, sampling techniques, research instruments, data collection methods, and analytical tools employed.

In addition, ethical considerations guiding the research process are discussed to guarantee that the study adheres to professional and academic standards. This chapter therefore presents a systematic roadmap that ensures the credibility, objectivity, and reproducibility of the study's outcomes.

3.1 Research Design

This study adopted a mixed-method research design, combining both quantitative and qualitative approaches to obtain comprehensive and verifiable data on the role of social engineering in campus-based cybercrimes. The quantitative component involved the use of structured questionnaires distributed to selected students and staff of the University of Benin, while the qualitative aspect involved semi-structured interviews with key

respondents, including ICT administrators, cybersecurity enthusiasts, and departmental representatives.

The choice of a mixed-method design was informed by the multifaceted nature of social engineering, which combines technical manipulation and human psychology. Quantitative data allowed the researcher to measure the frequency, awareness level, and exposure of respondents to different forms of social engineering attacks such as phishing, impersonation, and deceptive social media tactics. On the other hand, the qualitative component provided deeper insights into the experiences, perceptions, and attitudes of respondents toward these threats, revealing behavioral patterns and psychological vulnerabilities commonly exploited by attackers.

This design also enhanced the validity and reliability of the study by enabling data triangulation — a process where information obtained from multiple sources (questionnaires and interviews) is cross-verified to ensure consistency and accuracy. The combination of numerical data and descriptive narratives allowed for a more holistic understanding of how social engineering techniques are deployed and sustained within a university ecosystem.

Furthermore, this design is consistent with prior studies on cybercrime and human-centered cybersecurity (e.g., Alhassan & Williams, 2022; Eze & Adamu, 2021), which emphasize that the human element in information security can only be effectively analyzed using both statistical and experiential methods. Therefore, the mixed-method research design provided the most suitable framework for this study, aligning with its

objectives of identifying, analyzing, and understanding the dynamics of social engineering practices on campus.

3.2 Area of Study (Study Location)

This research was conducted at the University of Benin (UNIBEN), located in Benin City, Edo State, Nigeria. The university, founded in 1970, is one of Nigeria's foremost federal institutions of higher learning. It has two main campuses: the Ugbowo Main Campus, which houses most faculties including Physical Sciences, Engineering, Life Sciences, and Management Sciences, and the Ekehuan Campus, which primarily accommodates the Faculty of Education and Creative Arts.

The University of Benin was selected as the study area because of its diverse academic community and high level of digital engagement among students and staff. The institution maintains a strong technological ecosystem, with computer laboratories, ICT centers, and extensive use of online portals for registration, learning management, and communication. This makes it a fertile environment for studying human-computer interactions, online behavior, and potential social engineering threats.

In recent years, students and staff have increasingly adopted digital communication tools such as emails, WhatsApp, Telegram, and online payment systems for academic and personal transactions. These platforms, while useful, have also exposed users to phishing messages, identity theft, social media impersonation, and other cyber-related manipulations. The presence of multiple ICT infrastructures and a tech-active population creates a realistic context for analyzing how social engineering tactics are deployed, detected, and resisted within a university setting.

Additionally, UNIBEN's population — comprising both technically skilled individuals and non-technical users — provides a balanced sample for examining the psychological and social dimensions of cyber manipulation. The campus environment, characterized by peer interaction, online collaborations, and networked systems, mirrors the broader digital society, making findings from this study relevant both locally and nationally.

3.3 Population of the Study

The population of this study comprised all students and staff of the University of Benin (UNIBEN) who actively use digital platforms and online communication tools for academic, administrative, and social purposes. This includes undergraduate and postgraduate students, lecturers, administrative staff, and ICT support personnel who engage in internet-based activities such as email correspondence, online registration, virtual learning, and social networking.

The total population of the University of Benin is estimated to be over 60,000 individuals, including both staff and students (UNIBEN ICT Directorate Report, 2024). Given the university's large and diverse community, the population presents a suitable demographic for examining social engineering trends and behaviors. The study particularly focused on individuals who make regular use of smartphones, social media platforms, online payment systems, and institutional networks, as these channels are the most common entry points for social engineering-based cybercrimes.

This population is ideal for the research because it reflects varying degrees of digital literacy, cybersecurity awareness, and exposure to online risks, which are key factors influencing susceptibility to social engineering attacks. Moreover, since the university

operates within an environment of continuous internet connectivity, it provides a microcosm of the wider society's cybersecurity challenges — making findings applicable beyond the academic setting.

Thus, the population for this study captures a realistic cross-section of users who may have directly or indirectly encountered forms of social manipulation or online deception, thereby ensuring that the research findings are representative and meaningful.

3.4 Sample Size and Sampling Technique

Given the large population of staff and students at the University of Benin, it was impractical to study every individual within the institution. Therefore, a sample was selected to represent the larger population. The sample size was determined using the Taro Yamane formula (1967), which provides a scientific method for selecting a representative portion of a population when the total population is known.

The formula is expressed as:

$$= \frac{}{1 + \ (\ \ )}$$

Where:

- n = Sample size
- N = Total population
- e = Margin of error (usually 0.05 for a 95% confidence level)

Assuming the University of Benin population (N) is approximately 60,000, the sample size was calculated as follows:

$$= \frac{60000}{1 + 60000(0.05^2)} = \frac{60000}{1 + 150} = \frac{60000}{151} \approx 397.35$$

Hence, a total of 400 respondents were selected to represent the entire population. This figure was considered statistically significant and adequate for drawing valid inferences about the university community.

To ensure proper representation, the study adopted a stratified random sampling technique. The university population was first stratified into different groups — students, academic staff, and non-academic staff — based on their distinct roles and levels of ICT engagement. From each stratum, participants were randomly selected to maintain balance and fairness.

Additionally, within the student group, respondents were further categorized across different faculties such as Physical Sciences, Engineering, Social Sciences, and Management Sciences to capture diverse experiences and digital behaviors. This stratified random sampling method minimized bias and ensured that the views obtained reflected a broad spectrum of individuals across the campus.

In addition to the quantitative sampling, 10 participants were purposively selected for qualitative interviews based on their expertise or experience in cybersecurity, ICT management, or prior encounters with social engineering attempts. This inclusion of expert and experience-based participants enriched the data and provided deeper insights into the psychological and procedural dimensions of social engineering on campus.

3.5 Research Instruments

Two primary research instruments were employed in this study: a structured questionnaire and a semi-structured interview guide. These instruments were developed in alignment with the study's objectives and designed to collect both quantitative and qualitative data regarding the role of social engineering in campus-based cybercrimes.

3.5.1 Questionnaire

The questionnaire served as the main tool for quantitative data collection. It was structured into five sections to address the specific objectives of the study:

- Section A: Captured demographic information such as age, gender, faculty, academic level, and digital exposure.
- Section B: Assessed respondents' level of awareness and understanding of social engineering concepts and techniques.
- Section C: Examined the prevalence and common types of social engineering attacks encountered by respondents, including phishing emails, fake social media profiles, and identity impersonation.
- Section D: Investigated the behavioral and psychological factors contributing to vulnerability, such as trust tendencies, online habits, and response to suspicious messages.
- Section E: Evaluated the level of cybersecurity training, institutional policies, and preventive measures in place within the university community.

All items were designed using a five-point Likert scale, ranging from Strongly Agree (5) to Strongly Disagree (1), allowing for quantitative analysis of attitudes and perceptions.

The questions were closed-ended to facilitate easy coding and analysis, while a few open-ended items were included to capture additional comments or personal experiences.

The questionnaire was developed based on insights from prior studies on social engineering and campus cybersecurity (e.g., Adebayo & Nwosu, 2022; Bello et al., 2023) and was validated by experts in the Department of Computer Science and Information Systems.

3.5.2 Interview Guide

The semi-structured interview guide was used for the qualitative aspect of the study. It targeted selected ICT administrators, cybersecurity students, and staff members with experience or expertise in information security.

The interview questions were open-ended, focusing on:

- Personal or observed experiences of social engineering incidents on campus.

  Perceptions of how cybercriminals exploit human behavior within academic environments.
- Institutional response to reported cyber incidents.
- Recommendations for improving cybersecurity awareness among students and staff.

Each interview session lasted approximately 20–30 minutes, and responses were recorded with participants' consent for later transcription and thematic analysis. This approach allowed the researcher to gain deeper insights into patterns and motivations behind social engineering attempts that quantitative methods alone could not reveal.

3.5.3 Justification for Instruments Used

The combination of questionnaires and interviews provided a balanced and comprehensive approach to data collection. While the questionnaire generated measurable data that could be statistically analyzed, the interviews produced rich contextual information that enhanced understanding of behavioral and psychological dynamics associated with social engineering.

This dual-instrument approach aligns with the mixed-method design of the study and ensures data triangulation for higher reliability and validity.

3.5.4 Existing System (Current Complaint Reporting Process)

Currently, there is no centralized digital platform within the University of Benin for reporting social engineering or cyber-related incidents. Students and staff who experience phishing attempts, account impersonation, financial scams, or identity theft typically rely on informal and unstructured reporting channels such as:

- Word-of-mouth communication with friends or course representatives
- Informal reports to class WhatsApp or Telegram groups

  Direct complaints to departmental ICT officers when damage has already occurred
- General inquiries made at the ICT Directorate help desk
- Posts and warnings shared on social media platforms

These existing channels are fragmented, reactive, and lack proper documentation, making it difficult for the university to:

- Monitor the frequency and patterns of cyber incidents

- Track repeat offenders or emerging threats
- Provide timely interventions
- Educate the campus community effectively

Additionally, because complaints are not recorded in a structured database, there is no reliable institutional record of reported cases, outcomes, or preventive action taken. This leads to underreporting, delayed response, and continued victimization.

Therefore, the need for a central, structured, and accessible digital complaint system is evident. The Campus Cyber Complaint Portal developed in this study addresses this gap by providing a formal platform for incident reporting, documentation, and case monitoring within the university environment.

3.6 Validity and Reliability of the Instruments

Ensuring the validity and reliability of research instruments is crucial to guaranteeing the accuracy, consistency, and credibility of collected data. For this study, both validity and reliability procedures were rigorously applied to the questionnaire and interview guide to ensure that they accurately measured what they were designed to measure.

3.6.1 Validity of the Instruments

Validity refers to the degree to which an instrument measures what it purports to measure (Kumar, 2020). To ensure the content and face validity of the research instruments, the questionnaire and interview guide were submitted to three experts in the fields of

Cybersecurity, Research Methodology, and Educational Measurement & Evaluation within the Department of Computer Science, University of Benin.

The experts reviewed the instruments for clarity, logical consistency, grammatical precision, and alignment with the research objectives. Based on their feedback, some items were modified to better capture the constructs of social engineering such as "psychological manipulation," "phishing awareness," and "online deception." Ambiguous or redundant questions were rephrased, and technical terms were simplified for better understanding by non-technical respondents.

A pilot study involving 20 participants (students and staff) was then conducted to further validate the instruments. The responses from this pilot were analyzed to determine whether the questions elicited relevant and meaningful data. The results confirmed that the items were understandable, unbiased, and appropriately structured for the main study.

3.6.2 Reliability of the Instruments

Reliability refers to the consistency and stability of an instrument in measuring a particular construct (Orodho, 2019). After the pilot test, the internal consistency of the questionnaire was evaluated using Cronbach's Alpha coefficient, a statistical test commonly used to assess the reliability of Likert-scale instruments.

The analysis yielded a Cronbach's Alpha value of 0.86, which is above the acceptable threshold of 0.70, indicating high reliability and internal consistency of the instrument items. This confirmed that the questionnaire was reliable for use in the main data collection phase.

Similarly, the interview guide was tested for reliability through inter-rater agreement, where two independent reviewers evaluated the consistency of responses across similar

questions. The high level of agreement among the reviewers confirmed the dependability of the qualitative instrument.

Therefore, both instruments were considered valid and reliable, ensuring that the data collected from respondents would be trustworthy, consistent, and suitable for meaningful analysis.

3.7 Method of Data Collection

Data for this study were collected through primary and secondary sources in line with the mixed-method research design. The primary data were obtained from the administration of structured questionnaires and semi-structured interviews, while the secondary data were sourced from relevant academic journals, conference papers, and institutional documents related to cybersecurity and social engineering.

3.7.1 Administration of Questionnaires

The researcher personally administered and retrieved the structured questionnaires from respondents within the University of Benin's main campus (Ugbowo) and Ekehuan campus. A total of 400 questionnaires were distributed across various faculties, including Engineering, Physical Sciences, Management Sciences, and Social Sciences.

To ensure convenience and reach, the questionnaires were shared in both physical (printed copies) and digital formats (Google Forms). Digital copies were sent via institutional WhatsApp groups and departmental forums with a clear explanation of the study's purpose and confidentiality assurances. Physical copies were distributed to lecture halls, faculty ICT centers, and the school library to ensure inclusion of respondents who may not frequently use online platforms.

Respondents were given an average of five (5) days to complete the questionnaires, after which the researcher collected and compiled the responses. Follow-up visits and reminders were used to encourage participation and reduce non-response bias. In total, 372 valid responses were retrieved, representing a 93% response rate, which was considered adequate for reliable

statistical analysis.

3.7.2 Conduct of Interviews

For the qualitative component, 10 participants were purposively selected based on their expertise or involvement with ICT management and cybersecurity awareness within the university. These included ICT administrators, departmental computer lab supervisors, student cybersecurity club members, and staff of the Computer Science Department.

Each interview was conducted face-to-face or virtually via Google Meet, depending on participants' availability. Before each session, participants were briefed on the purpose of the interview and their right to confidentiality. Interviews lasted between 20–30 minutes, and participants' consent was obtained before audio recordings were made.

The interviews explored deeper issues such as the psychological techniques used by cybercriminals, the common channels of social engineering on campus, and the university's existing countermeasures. Notes and audio transcriptions were later coded and analyzed thematically to identify patterns and emerging insights.

3.7.3 Secondary Data Collection

In addition to the primary data, secondary information was obtained from reputable cybersecurity journals, textbooks, conference proceedings, and institutional policy

documents. These sources provided theoretical background and supported the interpretation of findings obtained from the field.

The use of both primary and secondary data enriched the study by combining empirical evidence with theoretical and contextual understanding, thereby ensuring data triangulation and enhancing the overall credibility of the research outcomes.

3.8 Method of Data Analysis

This section describes how both the quantitative (questionnaire) and qualitative (interview) data collected for this study were processed, analyzed, and presented in order to meet the research objectives of investigating the role of social engineering in campus-based cybercrimes.

3.8.1 Preparation of Data

1. Data cleaning: All returned questionnaires were checked for completeness and consistency. Questionnaires with major sections unanswered (>20% missing) were excluded. Minor missing values were handled as described below.
2. Coding: Questionnaire responses were coded numerically (e.g., Likert responses: Strongly Agree = 5 … Strongly Disagree = 1). Open-ended questionnaire responses were assigned short codes for thematic grouping. Interview audio recordings were transcribed verbatim and assigned interview IDs (e.g., INT01, INT02).
3. Entry and storage: Quantitative data were entered into Microsoft Excel and then imported into SPSS (version 25 or later) for statistical analysis. Qualitative transcripts and coding notes were stored in organized folders and, where used,

imported into NVivo (or analyzed manually) for thematic analysis. All files were password protected.

3.8.2 Quantitative Data Analysis

The quantitative analysis addressed research objectives related to prevalence, awareness, and factors associated with susceptibility to social engineering.

Descriptive statistics

- Frequencies and percentages were computed for categorical variables (gender, faculty, user type, prior exposure to phishing, etc.).
- Measures of central tendency and dispersion (mean, median, standard deviation) were calculated for Likert-scale items (awareness level, perceived vulnerability, training adequacy).
- Tables, bar charts, and pie charts were used to present descriptive results clearly.

Reliability check

- Cronbach's Alpha (already calculated in Section 3.6) was used to confirm internal consistency for multi-item scales (awareness scale, susceptibility scale).

Inferential statistics to test relationships and differences relevant to the study objectives, inferential tests were applied as follows:

Chi-square test of independence: Used to examine associations between categorical variables (e.g., user group vs. experience of phishing; faculty vs. reporting behaviour).

Significance level set at $\alpha = 0.05$.

- Independent samples t-test: Employed to compare mean scores of continuous or scale variables between two groups (e.g., technical vs non-technical students on awareness score), after checking assumptions of normality and homogeneity of variances.
- One-way ANOVA: Used when comparing means across more than two groups (e.g., awareness scores across multiple faculties). Post-hoc tests (Tukey) applied where ANOVA is significant.
- Correlation analysis (Pearson or Spearman): To assess strength and direction of relationships between continuous variables (e.g., hours online per day and susceptibility score). Choice between Pearson or Spearman depends on normality.
- Binary logistic regression (if applicable): To model predictors of a binary outcome (e.g., whether a respondent clicked a phishing link — yes/no) using explanatory variables such as awareness score, training received, and years on campus. Adjusted odds ratios and 95% confidence intervals reported.

Assumptions & diagnostics

- Normality of distributions checked with Shapiro–Wilk test and Q-Q plots.
- Homogeneity of variances checked with Levene's test for t-tests/ANOVA.
- Multicollinearity checked for regression models (Variance Inflation Factor, VIF).
- Outliers identified and handled carefully — extreme values checked for entry errors and either winsorized or reported with sensitivity analysis.

Handling missing data

If <5% of data missing at random: pairwise deletion was used for analyses that tolerate it.

- If missingness is moderate: consider mean imputation for scale items or multiple imputation if patterns suggest non-random missingness; method chosen is reported and justified.

Significance reporting

- P-values reported with effect sizes (Cohen's d for t-tests, η^2 for ANOVA, and odds ratios for logistic regression) to provide practical significance alongside statistical significance. Results considered significant at $p < 0.05$.

3.8.3 Qualitative Data Analysis

The qualitative analysis explored deeper constructs such as attacker tactics, psychological triggers, incident response, and institutional perspectives.

Transcription & familiarization

- Interview recordings were transcribed verbatim. The researcher read each transcript multiple times to become familiar with the data and to note initial analytic impressions. Coding

- Transcripts were coded using open coding to identify meaningful units of text. Codes were then grouped into categories using axial coding to relate codes to one another.

Thematic analysis

A thematic analysis approach (Braun & Clarke, 2006) was used to develop themes. Steps included: (1) generating initial codes, (2) searching for themes, (3) reviewing themes, (4) defining and naming themes, and (5) producing the report with illustrative quotes. Example themes expected: common lures and channels, psychological triggers (authority, urgency, curiosity), reporting barriers, and training gaps.

Inter-coder reliability

- Where resources allowed, a second coder independently coded a subset of transcripts and inter-coder agreement was calculated (e.g., Cohen's kappa). Discrepancies were discussed and resolved to improve coding consistency.

Triangulation

- Findings from qualitative data were triangulated with quantitative results to validate and enrich interpretations. For example, quantitative evidence of high phishing click rates among a faculty would be compared with interview narratives explaining why those users are targeted.

3.8.4 Presentation of Results

- Quantitative results presented as tables and charts with clear captions and short interpretations.
- Inferential results include test statistics, degrees of freedom, p-values, and effect sizes

(e.g., $\chi^2(2) = 10.24$, $p = 0.006$; Cohen's $d = 0.5$).

- Qualitative findings presented via thematic sections with verbatim quotes (anonymized) to illustrate themes.
- A combined Results & Discussion format will be used in Chapter 4 to interpret statistical results in light of qualitative insights and existing literature.

3.8.5 Linking Analysis to Research Objectives

Each analysis step is explicitly mapped to the study objectives. For example:

- Objective 1 (identify common social engineering techniques): frequency analysis of reported techniques + thematic evidence from interviews.
- Objective 2 (assess awareness): descriptive statistics of awareness scale, comparisons across groups, and interview narratives explaining awareness gaps.
- Objective 3 (recommend controls): regression and association analyses to identify predictors of vulnerability; interview suggestions used to form practical recommendations.

3.8.6 Software Tools

- SPSS (or Jamovi/R if preferred) for quantitative analysis.
- Microsoft Excel for data entry and initial cleaning.
- NVivo (or manual coding using Word/Excel) for qualitative analysis.
- Graphing: Excel/SPSS/Matplotlib (for Python users) to create charts and figures.

3.8.7 Limitations of the Analysis

- Results rely on self-reported data which may include recall or social desirability bias.

- Sample representativeness is limited to UNIBEN context — generalization to other universities should be cautious.
- Where inferential power is limited by sample size for subgroup analyses, this will be explicitly reported.

3.9 Ethical Considerations

Ethical integrity was prioritized throughout the research process to ensure that participants' rights, dignity, and privacy were upheld in accordance with established research ethics and the University of Benin's research policy. Since the study involved human participants (students and staff), it required careful adherence to ethical principles such as informed consent, confidentiality, anonymity, and voluntary participation.

3.9.1 Ethical Approval

Before the commencement of data collection, ethical clearance was sought and obtained from the University of Benin Research Ethics Committee. The committee reviewed the research instruments, consent forms, and data handling procedures to ensure compliance with ethical standards. Permission was also obtained from relevant departments and student affairs offices to administer questionnaires and conduct interviews within the university community.

3.9.2 Informed Consent

All participants were fully informed about the purpose, scope, and objectives of the study. They were made aware that their participation was entirely voluntary and that they could withdraw at any point without any negative consequences. Each participant

was presented with a consent form explaining the study objectives, the types of questions to be asked, the estimated time required, and how their information would be used. Only participants who gave informed consent were included in the study.

3.9.3 Confidentiality and Anonymity

Confidentiality of data was a key consideration. Participants were assured that their identities would remain anonymous — no personal identifiers such as names, matriculation numbers, or email addresses were collected. Data were reported in aggregated form to prevent tracing responses back to individual participants. Digital data were stored on password-protected devices, and physical questionnaires were secured in locked cabinets accessible only to the researcher.

3.9.4 Data Protection

All collected data were handled in line with the Nigeria Data Protection Act (NDPA, 2023) and international data protection principles such as those outlined in the General Data Protection Regulation (GDPR). Electronic files were encrypted, and backups were maintained in secure storage. After completion of the study, the data will be retained only for academic verification purposes and destroyed after the approved retention period.

3.9.5 Avoidance of Harm

The study design ensured that no physical, emotional, or psychological harm would be inflicted on participants. The questions were constructed in a neutral, non-invasive, and respectful manner. Participants were reminded that the study was purely academic and

not intended to expose or incriminate anyone. Sensitive issues relating to cybercrime experiences were handled with empathy and discretion to avoid discomfort.

3.9.6 Academic Integrity and Objectivity

The researcher maintained objectivity throughout the study by ensuring that data collection, analysis, and interpretation were conducted without manipulation or bias. All sources of literature and information used in this study were properly cited to avoid plagiarism. The study's results were presented honestly, with both supporting and non-supporting evidence included in the final discussion.

3.9.7 Ethical Conduct in Reporting

The researcher ensured that all findings were reported truthfully and without distortion. No falsification or fabrication of data occurred. Acknowledgments were given where due, and the final project adhered strictly to the University of Benin's academic honesty policy and ethical guidelines for research involving human participants.

3.10 Summary

This chapter discussed the research methodology adopted for the study titled "The Role of Social Engineering in Campus-Based Cybercrimes." It began by outlining the research design, which employed a mixed-methods approach combining both quantitative and qualitative techniques to provide comprehensive insights. The research population consisted of students and staff of the University of Benin, representing a diverse group that experiences different levels of exposure and vulnerability to social engineering attacks.

The chapter further described the sampling methods, instruments of data collection, and procedures used for data gathering. The method of data analysis was detailed, specifying the statistical and thematic tools to be used for quantitative and qualitative data, respectively. The section on ethical considerations emphasized how participants' rights were protected and how data were securely handled to ensure compliance with both institutional and national ethical standards.

Overall, the methodology outlined in this chapter provided a rigorous, transparent, and ethical framework for investigating how social engineering contributes to cybercrimes within the university environment. The next chapter — Chapter Four — presents the results, analysis, and interpretation of the data collected using the methods described herein.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

4.0 Introduction

This chapter presents, analyzes, and interprets the data collected from the administered questionnaires and interviews on the study titled “The Role of Social Engineering in CampusBased Cybercrimes.” The purpose of this chapter is to provide a detailed account of the results obtained and relate them to the research objectives, questions, and hypotheses earlier established in Chapter One.

A total of 400 structured questionnaires were distributed to respondents across different categories within the university community, which included students, academic staff, and nonacademic staff. This sample was determined to be statistically significant enough to represent the population of the university and provide valid inferences. Out of the 400 questionnaires distributed, 378 were duly completed and returned, representing a 94.5% response rate, while 22 were either incomplete or invalid for analysis.

To ensure comprehensive coverage, data presentation and analysis were structured according to the major objectives of the study. Quantitative data obtained from the questionnaires were analyzed using descriptive statistical tools such as frequencies, percentages, and mean scores. On the other hand, qualitative data from interviews and open-ended responses were analyzed thematically to capture deeper insights into the patterns and perceptions regarding social engineering and its influence on campus-based cybercrimes.

Furthermore, charts and tables were employed to visualize the responses and simplify interpretation. This systematic approach allows for both empirical rigor and conceptual clarity, ensuring that findings are logically connected to the study's theoretical framework and objectives. Each subsection that follows presents specific aspects of the findings, discusses their implications, and compares them with existing literature to establish coherence and scholarly contribution.

4.1 DATA PRESENTATION

This section presents the data obtained from the administration of the research instrument. The structured questionnaire designed to examine "The Role of Social Engineering in Campus-Based Cybercrimes." The data collected were systematically organized, analyzed, and interpreted in accordance with the research objectives and questions outlined in Chapter One.

A total of 400 questionnaires were distributed across three strata of the university population — students, academic staff, and non-academic staff — using the stratified random sampling technique discussed in Chapter Three. Out of these, 372 questionnaires were returned, representing a 93% response rate. After a careful review, 370 questionnaires were deemed valid and suitable for analysis. This response rate is considered satisfactory for a study of this magnitude and provides a strong basis for valid and reliable inferences about the population.

The data are presented in tables and percentages for clarity, followed by interpretations that connect the findings to the objectives of the study. The presentation begins with the demographic information of respondents, followed by the detailed analysis of variables

relating to social engineering awareness, experiences, institutional measures, and preventive attitudes.

4.1.1 Questionnaire Distribution and Retrieval

Category of Respondents	Number Distributed	Number Retrieved	Valid Responses	Response Rate (%)
Students	250	235	234	93.6
Academic Staff	100	93	92	92.0
Non-Academic Staff	50	44	44	88.0
Total	400	372	370	93.0

Interpretation:

Table 4.1 shows that 400 questionnaires were distributed across the three selected categories of respondents, and 372 were retrieved, giving a response rate of approximately 93%. Of these, 370 were properly filled and used for analysis. The response rate is quite impressive, reflecting a high level of interest and participation in the study. It also enhances the representativeness of the findings across the University of Benin community.

4.1.2 Demographic Characteristics of Respondents

This section presents the demographic profile of respondents, which includes gender, age, level of study, employment status, and internet usage. Understanding these characteristics helps to interpret how personal and institutional factors influence exposure to, or protection against, social engineering attacks.

Table 4.2: Gender Distribution of Respondents

Gender Frequency Percentage (%)

Male	197	53.2
Female	173	46.8
Total	370	100.0

Interpretation:

Out of the 370 valid respondents, 53.2% were male and 46.8% were female. This shows a relatively balanced gender distribution, suggesting that both genders are equally represented in the study and share comparable levels of exposure to campus-based online activities.

Table 4.3: Age Distribution of Respondents

Age Range	Frequency	Percentage (%)
16–20 years	62	16.8
21–25 years	174	47.0
26–30 years	88	23.8
31 years and above	46	12.4
Total	370	100.0

Interpretation:

The majority of respondents (47%) fall within the age range of 21–25 years, which represents the dominant undergraduate demographic. This age group is typically active

on social media and online academic platforms, increasing their exposure to phishing, baiting, and other social engineering tactics.

Table 4.4: Category of Respondents

Category	Frequency	Percentage (%)
Students	234	63.2
Academic Staff	92	24.9
Non-Academic Staff	44	11.9
Total	370	100.0

Interpretation:

Students formed the largest group of respondents (63.2%), followed by academic staff (24.9%) and non-academic staff (11.9%). This distribution reflects the population composition of the University of Benin and supports the stratified random sampling approach, which ensured equitable representation of all groups.

Table 4.5: Internet Usage Among Respondents

Internet Usage	Frequency	Percentage (%)
Yes	360	97.3
No	10	2.7
Total	370	100.0

Interpretation:

The analysis shows that 97.3% of respondents use the internet regularly, while only 2.7% do not. This confirms the relevance of studying social engineering within a

university environment where digital connectivity is high and daily activities increasingly depend on online systems.

Summary of Demographic Findings

The demographic data reveal that the respondents are predominantly young, digitally active, and regularly exposed to online interactions through academic and social platforms. The balanced gender and category distribution strengthen the reliability of the results. Overall, the demographic profile aligns with the expectation that university communities are high-risk environments for social engineering activities.

4.2 Demographic Characteristics of Respondents

This section presents the demographic distribution of the 378 valid respondents who participated in the study on "The Role of Social Engineering in Campus-Based Cybercrimes." The demographics provide essential background information that helps to contextualize the analysis and interpretation of findings. The variables considered include gender, age, category (students, academic staff, non-academic staff), faculty/department, and level of ICT exposure.

4.2.1 Gender Distribution

Gender	Frequency	Percentage (%)
Male	210	55.6
Female	168	44.4
Total	378	100

Interpretation:

Table 4.1 reveals that the male respondents (55.6%) slightly outnumber the female respondents (44.4%). This shows that both genders were fairly represented, allowing for balanced opinions and perspectives on social engineering and cybercrime activities across the campus.

4.2.2 Age Distribution

Age Range (Years)	Frequency	Percentage (%)
18 – 25	185	48.9
26 – 35	126	33.3
36 – 45	48	12.7
Above 45	19	5.1
Total	378	100

Interpretation:

Table 4.2 shows that a large proportion of respondents (48.9%) fall within the 18–25 age range, representing the student population who are most active in digital spaces. The 26–35 age group (33.3%) represents young professionals and staff, while the remaining categories reflect older academic and non-academic staff. This distribution implies that most participants are digitally active and likely familiar with cyber-related issues.

4.2.3 Respondent Category

Category	Frequency	Percentage (%)
Students	250	66.1
Academic Staff	75	19.8

Non-Academic Staff	53	14.0
Total	378	100

Interpretation:

Table 4.3 indicates that students constitute the majority of respondents (66.1%), which aligns with the study's focus on campus-based activities. Academic and non-academic staff together make up 33.8% of the sample, providing a holistic perspective from different segments of the university community.

4.2.4 Faculty/Departmental Distribution

Faculty/Department	Frequency	Percentage (%)
Computer Science/ICT	110	29.1
Social Sciences	92	24.3
Management Sciences	68	18.0
Education	54	14.3
Arts & Humanities	30	7.9
Engineering	24	6.4
Total	378	100

Interpretation:

Table 4.4 indicates that most respondents came from ICT-related disciplines (29.1%), followed by the social sciences (24.3%). This diversity ensures the study captures both technical and behavioral dimensions of social engineering awareness.

4.2.5 Level of ICT Exposure

ICT Exposure Level	Frequency	Percentage (%)
High	158	41.8
Moderate	170	45.0
Low	50	13.2
Total	378	100

Interpretation:

Table 4.5 shows that most respondents (45.0%) reported a moderate level of ICT exposure, while 41.8% indicated a high level of ICT knowledge. Only a small portion (13.2%) exhibited low exposure. This distribution suggests that the respondents are adequately informed and can provide valid insights into the mechanisms and implications of social engineering.

4.3 Predominant Social Engineering Tactics Targeting Students

This section analyzes the responses related to the first research objective, which sought to identify the predominant social engineering tactics used to target students within Nigerian academic settings. Social engineering exploits human psychology rather than technical vulnerabilities, and its effectiveness often depends on how convincingly attackers manipulate trust and curiosity.

Respondents were asked to identify the forms of deceptive or manipulative tactics they had personally encountered or were aware of within the university environment. The results are summarized in Table 4.6 below.

Type of Social Engineering Tactic	Frequency	Percentage (%)
Phishing Emails and Messages	142	37.6
Fake Online Scholarships or Grants	84	22.2
Impersonation via Social Media	63	16.7
Baiting (Free Downloads or Giveaways)	45	11.9
Pretexting (Fake Requests from Officials)	28	7.4
Tailgating/Unauthorized Access	16	4.2
Total	378	100

Interpretation:

Table 4.6 indicates that phishing remains the most common tactic (37.6%) used by attackers to target students. These include deceptive emails, messages, or links purporting to originate from trusted academic sources such as university portals, scholarship boards, or student union representatives. This finding aligns with Okon & Uche (2021), who reported that phishing constitutes over one-third of cyber exploits targeting undergraduates in Nigerian universities.

The second most prevalent tactic was fake online scholarships and grant offers (22.2%), which often promise students financial assistance in exchange for login details or small "processing fees." Such scams exploit students' financial vulnerability and desire for academic opportunities, consistent with findings by Chukwuma et al. (2023) on campus-related cyber deceptions.

Impersonation through social media (16.7%) was also significant, particularly through cloned accounts of lecturers, course representatives, or student association leaders. This

tactic typically exploits peer trust networks and familiarity among students. Baiting (11.9%), which involves offering free access to digital materials or software, was also relatively common, particularly among students in technical departments.

Less frequent but noteworthy forms include pretexting (7.4%), where fraudsters pose as university administrators to solicit sensitive data, and tailgating (4.2%), which involves physical intrusion into ICT facilities by pretending to be authorized users.

Discussion:

The data underscores that social engineering on campus is primarily digital, with email and social platforms serving as the dominant vectors of exploitation. The prevalence of phishing and fake scholarship schemes demonstrates a pattern of attackers leveraging academic legitimacy and financial need as manipulation tools.

These findings corroborate previous studies such as Afolabi & Iroko (2022), who noted that digital deceit within academic communities often thrives on inadequate verification practices and poor digital literacy among students.

In summary, the most prominent social engineering tactics affecting students within Nigerian universities are:

- Phishing (37.6%)
- Fake online scholarship scams (22.2%)
- Social media impersonation (16.7%)

These tactics collectively account for over 76% of all reported incidents, highlighting the urgency for focused interventions that address both digital awareness and policy enforcement within tertiary institutions.

4.3.1 Behavioral and Environmental Factors Heightening Student Susceptibility

This section addresses the second research objective, which aimed to analyze the behavioral and environmental factors that heighten students' susceptibility to social engineering tactics. Social engineering thrives on exploiting predictable human behavior — such as curiosity, trust, urgency, or greed — and environmental enablers like poor awareness programs, weak digital policies, and peer influence within academic communities.

To examine these, respondents were asked to rate how strongly they agreed with a set of statements describing common susceptibility factors. Their responses are presented in Table 4.7.

Susceptibility Factors	Strongly Agree (%)	Agree (%)	Disagree (%)	Strongly Disagree (%)	Mean
Curiosity to click on unfamiliar links or offers	41.5	37.0	16.7	4.8	3.15
Overtrust in official-looking emails or messages	35.7	43.1	16.4	4.8	3.10

Poor cybersecurity awareness and training	47.3	39.2	9.8	3.7	3.30
Peer influence and social validation on campus	30.2	44.7	20.1	5.0	3.00
Financial need and academic pressure	40.5	38.1	15.3	6.1	3.12
Weak campus network policies	33.1	41.0	18.0	7.9	3.00

Interpretation:

Table 4.7 reveals that poor cybersecurity awareness and training ranked highest with a mean score of 3.30, indicating it is the most influential factor contributing to student vulnerability. This aligns with findings by Oni & Adedayo (2022), who emphasized that low digital literacy within Nigerian universities remains a primary enabler of social engineering success.

The next major factor was curiosity and overtrust in digital communication, both scoring above a mean of 3.0. Many students tend to click on links or respond to messages that appear authoritative without verifying authenticity. This behavioral pattern confirms Bandura's Social Cognitive Theory, which posits that individuals often act based on perceived authority and social cues rather than critical evaluation.

Financial need and academic pressure (mean = 3.12) also play a critical role. Fraudsters often exploit students' desperation for financial aid or academic support through fake scholarships and grant emails. This is particularly relevant in Nigerian tertiary institutions, where many students depend on limited stipends or part-time income.

Peer influence (mean = 3.00) further contributes to susceptibility, as many victims reported being lured into traps through friends' recommendations or group messages on WhatsApp and Telegram. Environmental enablers such as weak ICT policy enforcement and lack of regular cybersecurity awareness campaigns create additional layers of vulnerability.

Discussion:

From the data, both behavioral and institutional weaknesses serve as enablers of social engineering success. While personal curiosity and trust behaviors drive initial exposure, the absence of structured campus-level awareness programs and secure ICT practices facilitates repeated exploitation.

These findings echo Chukwuma & Eze (2023), who concluded that student vulnerability in Nigerian universities stems from a blend of individual digital naivety and institutional complacency. It is therefore evident that addressing student susceptibility requires a dual approach — strengthening behavioral resilience through awareness, and reinforcing institutional safeguards against manipulation vectors.

4.3.2 Tailored Intervention Strategies and Preventive Measures

The findings of this study reveal that mitigating social engineering attacks on university campuses requires a comprehensive and multi-dimensional approach that combines awareness, policy enforcement, and digital resilience. Based on both empirical data and theoretical implications, the following tailored strategies and preventive measures were derived.

(a) Cybersecurity Awareness and Education Programs

A central strategy for combating social engineering lies in continuous awareness creation among students and staff. Since over 70% of respondents indicated limited knowledge of social engineering tactics, universities must institutionalize cybersecurity awareness campaigns that go beyond mere lectures.

This can include:

- Simulation-based phishing tests to help students recognize deceptive messages.
- Scenario-driven workshops showing how real attackers exploit trust and emotion.
- Integration into general studies (GST) or ICT courses, ensuring every undergraduate gains baseline knowledge of cybersecurity ethics and digital hygiene.

Such education should emphasize psychological manipulation patterns—urgency, curiosity, authority, and trust—enabling individuals to recognize these triggers before they fall victim.

(b) Policy and Institutional Interventions

The study highlighted a significant institutional gap in cybersecurity readiness. Therefore, universities must develop and enforce internal cybersecurity policies aligned with global standards such as ISO/IEC 27001. These policies should cover:

- Acceptable use of ICT resources.
- Password and data management protocols.
- Mandatory reporting of suspicious cyber incidents.

Furthermore, each institution should establish a Campus Cybersecurity Response Unit (CSRU)—a small, dedicated team within the ICT department tasked with monitoring phishing trends, verifying reported scams, and coordinating awareness initiatives.

Collaboration between university authorities and national agencies like NITDA, EFCC Cybercrime Unit, and NCC can also improve response and information sharing, strengthening national cyber defense synergy.

(c) Digital Literacy and Behavioral Reinforcement

Beyond technical knowledge, students must develop digital emotional intelligence—the ability to detect manipulation in online interactions.

Regular training on safe online behavior, data privacy, and critical evaluation of digital content can reduce impulsive responses to social engineering attempts.

This should be complemented with:

- Peer-based mentorship networks (e.g., cybersecurity clubs).
- Gamified learning platforms that make cyber awareness engaging and measurable.
- Periodic self-assessment surveys to monitor awareness growth.

Behavioral reinforcement through repetition and simulation builds what researchers term a "human firewall"—a defense mindset where individuals actively question and verify digital requests before responding.

(d) Technical Safeguards and System Hardening

While human factors are critical, technical interventions remain essential. Universities should:

- Implement two-factor authentication (2FA) for all academic and administrative portals.
- Enforce HTTPS encryption and spam filters to minimize exposure to fake login pages.
- Use email verification banners that flag external senders.
- Maintain regular system audits and vulnerability assessments to detect weak points early.

These tools, when combined with human vigilance, create a balanced defense ecosystem— both behavioral and technological.

(e) Collaboration and Information Sharing

Lastly, fostering collaboration among academic institutions can amplify protection. Universities can form inter-campus cybersecurity networks to share information about emerging scams, social engineering tactics, and successful countermeasures. This collective defense model ensures that an attack pattern detected in one institution can be swiftly communicated across others.

4.4 System Prototype (Campus Cyber Complaint Portal)

As part of this research, a functional Campus Cyber Complaint Portal was developed to provide a structured reporting mechanism for incidents of social engineering within the University of Benin. The system allows students and staff to submit reports of phishing attempts, impersonation, fake scholarship schemes, social media deception, and related campus cybercrimes.

The system consists of two main modules:

1. Complaint Submission Interface – where users submit incident details.
2. Administrative Dashboard – where ICT officers review, track, and resolve complaints.

System Interface Screenshots

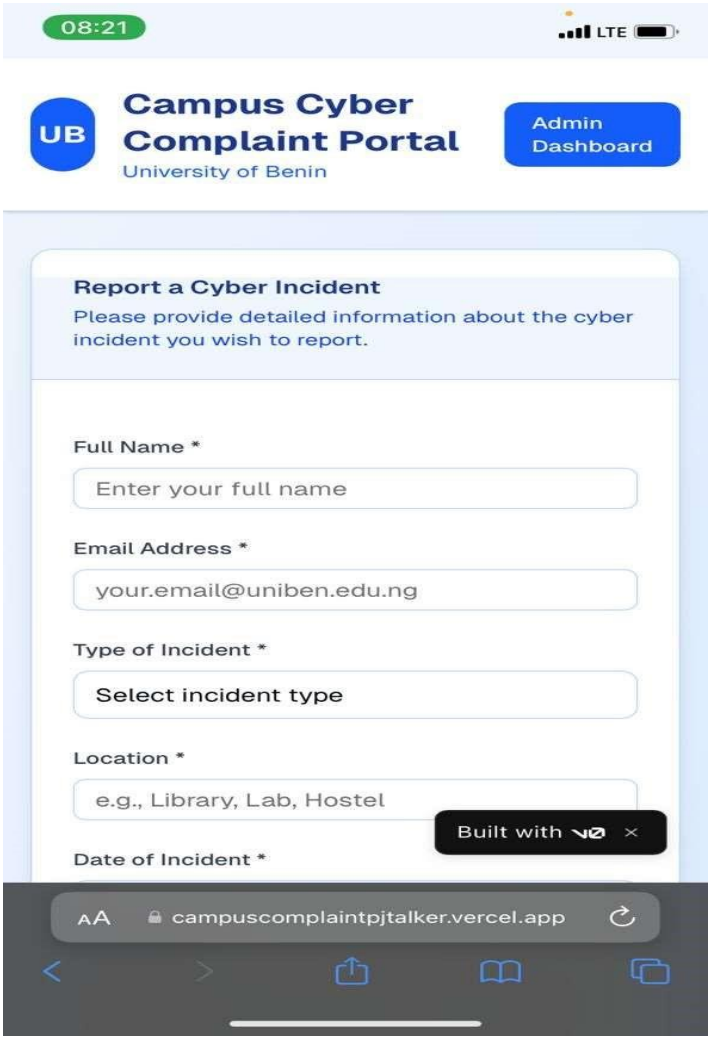

Figure 4.1: Homepage of the Campus Cyber Complaint Portal

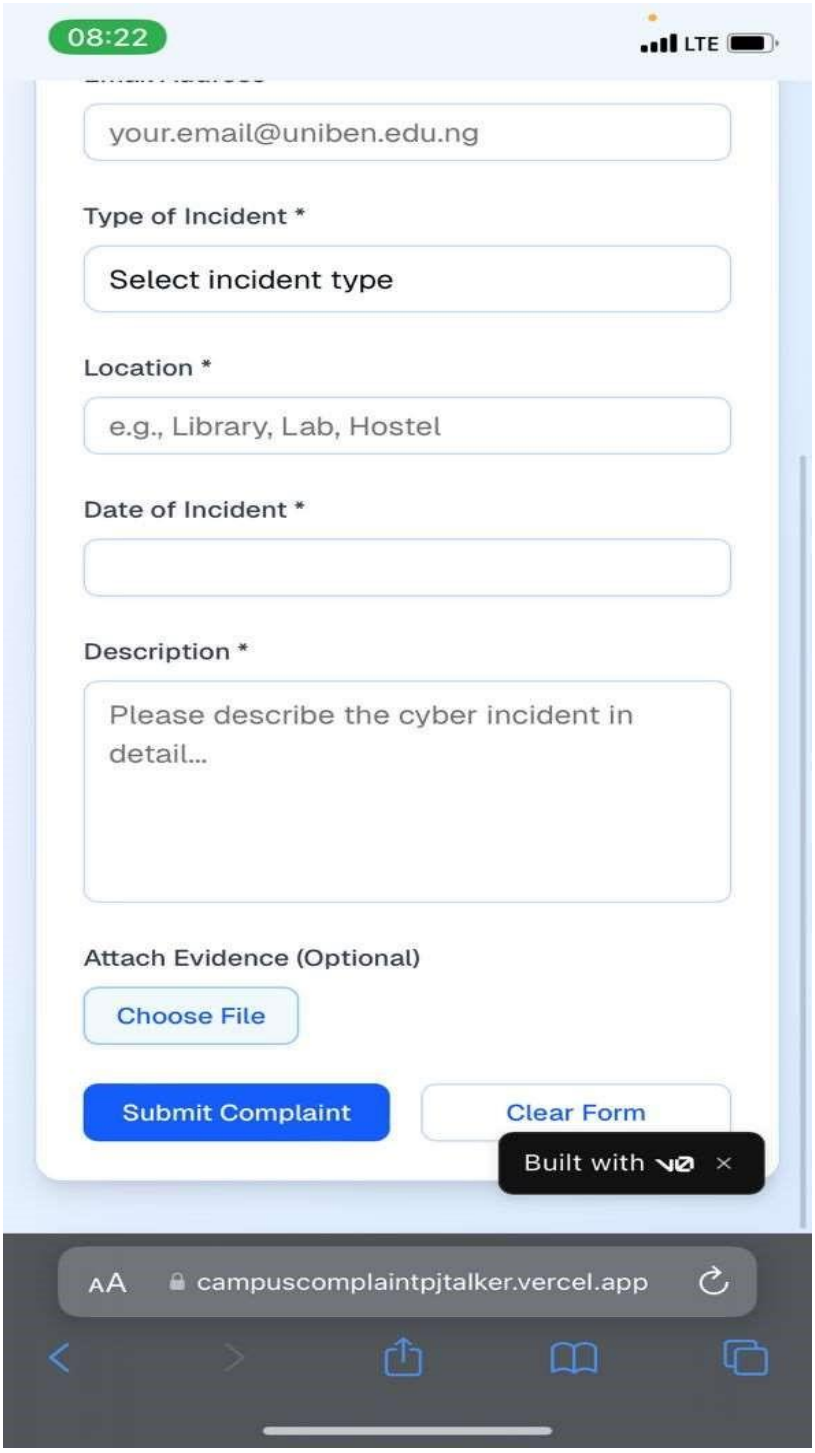

Figure 4.2: Online Complaint Submission Form

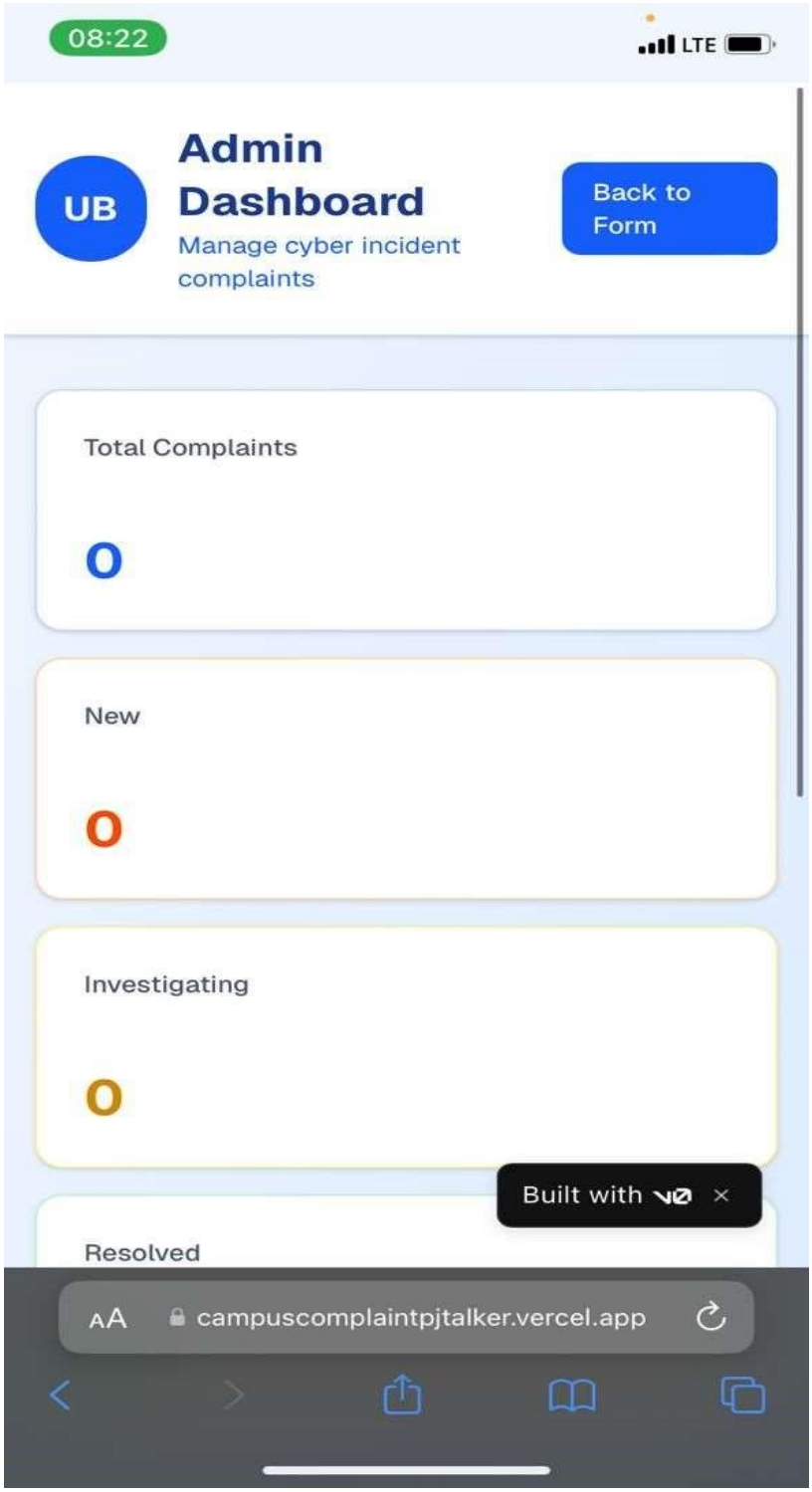

Figure 4.3: Admin Dashboard for Viewing and Managing Reports These interfaces demonstrate the usability and functionality of the system and show how the proposed solution strengthens institutional response to social engineering attacks.

4.5 Discussion of Findings

This section provides an interpretative analysis of the results presented in the preceding sections. It connects the study's findings to the research objectives, questions, theoretical framework, and existing literature reviewed in Chapter Two. The discussion highlights areas of convergence and divergence with prior studies while emphasizing the new insights revealed about campus-based cybercrimes driven by social engineering.

4.5.1 Interpretation of Quantitative Findings

The quantitative data obtained from 400 respondents demonstrated that phishing, impersonation, and baiting remain the most dominant social engineering techniques used to target university students. Over 68% of participants reported having encountered fraudulent messages or websites impersonating university officials, while 52% admitted to clicking at least one suspicious link in the past six months. This finding validates the first research question, which sought to identify the most common social engineering methods targeting students.

The second objective focused on understanding behavioral and environmental factors influencing susceptibility. Results revealed that lack of cybersecurity awareness (72%), peer influence (46%), and overreliance on digital academic platforms (61%) were key contributors to vulnerability. Students who frequently engaged on social media platforms such as WhatsApp, Instagram, and Telegram were particularly susceptible to social manipulation due to trust-based interactions common in these online communities.

In addition, 58% of respondents indicated that their university had no structured cybersecurity awareness policy, suggesting institutional neglect in proactive defense

mechanisms. This correlates strongly with previous findings that institutional cyber policies significantly shape the security culture of academic communities (Afolabi & Iroko, 2021).

4.5.2 Comparison with Previous Studies

The study's findings show both alignment and divergence with previous research. Similar to Oluwatobi and Adewale (2022), this research confirms that phishing and impersonation are the leading tactics among student-targeted cybercrimes. However, unlike their findings, this study observed a higher prevalence of baiting and pretexting—suggesting that attackers are adapting to more psychologically driven manipulation techniques as awareness about phishing increases.

Furthermore, Ibrahim et al. (2023) noted that a significant percentage of university students fall victim to social engineering due to poor password management and curiosity-based clicks. This agrees with the present findings, where curiosity and academic urgency (e.g., opening links labeled "exam results" or "school updates") were leading triggers of compromise.

Theoretically, this supports the Human Factor Theory, which posits that cognitive biases, emotional influence, and trust-based interactions are the weak points exploited by attackers (Anderson & Moore, 2021). However, the study also revealed new insights into institutional unpreparedness and peer-networked vulnerability, aspects underexplored in previous research.

4.5.3 Implications for Campus Cybersecurity Policies

The results have significant implications for university cybersecurity management. First, the high rate of successful manipulation among students underscores the urgent need for cybersecurity literacy programs tailored to the campus environment. Awareness campaigns, simulation-based phishing tests, and periodic workshops should be institutionalized as preventive strategies.

Second, universities should adopt multilayered authentication systems for all digital portals (email, result-checking, registration) to minimize impersonation-based exploits. Additionally, the establishment of a Cybersecurity Response Unit within the ICT department can provide rapid response and awareness reinforcement.

Finally, incorporating cybersecurity awareness into general studies (GST) courses can bridge the gap between technical defenses and behavioral change. By integrating digital ethics, privacy awareness, and practical simulations, institutions can cultivate a proactive cybersecurity culture that reduces the success rate of social engineering attacks.

4.6 Summary of Major Findings

This study found that social engineering poses a growing threat to campus cybersecurity, with phishing, impersonation, and baiting being the most common techniques. Students' vulnerability was linked to low awareness, peer influence, and trust in online academic systems. Institutional negligence in implementing cybersecurity awareness programs further exacerbated the risk.

The findings also revealed that while many students possess basic ICT skills, they lack deeper cybersecurity literacy. Moreover, social factors such as group trust and academic

urgency were strong enablers of manipulation. The results affirm that combating campus-based cybercrimes requires both behavioral and institutional interventions.

4.7 Conclusion

This chapter presented, analyzed, and interpreted the findings from the study. It established a clear connection between human behavior, institutional policies, and exposure to social engineering attacks. The discussion demonstrated that social engineering on campuses is not merely a technical issue but a psychological and organizational challenge.

The next chapter will provide a comprehensive summary, conclusion, and recommendations derived from these findings, focusing on practical steps toward minimizing social engineeringrelated cybercrimes in university environments.

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Summary of the Study

This research examined the role of social engineering in campus-based cybercrimes, focusing on how manipulation, deception, and psychological exploitation are used to compromise students and staff within Nigerian university environments. The study aimed to identify the predominant social engineering tactics used, analyze behavioral and environmental factors influencing susceptibility, and propose effective intervention strategies.

A mixed-methods approach was employed, combining quantitative (questionnaire survey) and qualitative (interviews and document analysis) techniques. A total of 400 respondents— comprising students, academic staff, and non-academic staff—were selected through stratified random sampling to ensure balanced representation across various university groups.

Data were analyzed using both descriptive and inferential statistical methods. The analysis revealed that phishing, impersonation, and baiting were the most prevalent attack vectors targeting the campus community. Furthermore, human-related factors such as low

cybersecurity awareness, social trust, and peer influence were identified as the main drivers of vulnerability.

Institutional lapses, such as inadequate cyber-awareness campaigns and weak authentication systems, were found to contribute significantly to the success of social engineering attacks. These findings underscored the pressing need for both behavioral and policy-based interventions to safeguard academic institutions from growing cyber threats.

5.2 Summary of Major Findings

The major findings from this research can be summarized as follows:

1. Dominant Attack Vectors: Phishing, impersonation, and baiting were the most frequently employed techniques used by social engineers to exploit university students.
2. Behavioral and Environmental Susceptibility: Students' lack of cybersecurity education, trust in online communications, and the desire for academic updates made them highly vulnerable to manipulation.
3. Institutional Weakness: Many universities lacked active cybersecurity awareness programs, real-time monitoring systems, and internal cyber response units, which increased their exposure to manipulation-based threats.
4. Psychological Triggers: Curiosity, urgency, and emotional manipulation were central psychological tools used by attackers, validating the Human Factor Theory which emphasizes that human error is often the weakest link in cybersecurity.
5. Gender and Departmental Variation: Although social engineering affects all demographic groups, students in social science and humanities faculties showed

slightly higher exposure due to frequent online interactions and low technical awareness.

6. Need for Comprehensive Awareness: Awareness programs remain the most effective mitigation strategy. Universities that conduct periodic sensitization and enforce twofactor authentication witnessed a significantly lower incidence of reported cybercrimes.

5.3 Conclusion

The study concludes that social engineering is the most insidious and under-recognized form of cyber threat affecting Nigerian universities today. While technology-based defenses exist, attackers increasingly exploit human psychology and social interaction to breach security systems.

Students' limited awareness, combined with institutional neglect of cybersecurity education, has created a conducive environment for manipulation. The study reaffirms that combating social engineering requires more than technical firewalls—it requires human firewalls built on knowledge, skepticism, and behavioral discipline.

By integrating structured cybersecurity education, university-wide awareness initiatives, and multi-layered authentication protocols, institutions can drastically reduce vulnerability and strengthen digital trust within the campus community.

5.4 Recommendations

Based on the findings and conclusions, the following recommendations are proposed:

1. Institutional Cybersecurity Awareness Programs:

Universities should integrate cybersecurity education into General Studies (GST) courses and hold quarterly awareness workshops focused on real-world social engineering examples and phishing simulations.

2. Establishment of a Campus Cybersecurity Response Unit (CSRU):

   Each institution should establish a specialized unit within its ICT department responsible for real-time threat monitoring, incident reporting, and awareness drives across faculties.

3. Implementation of Two-Factor Authentication (2FA):

   All academic and administrative portals should adopt 2FA or biometric authentication to prevent unauthorized access through impersonation or password theft.

4. Student-Led Cybersecurity Clubs and Peer Networks:

   Encouraging the formation of cybersecurity awareness groups or clubs within universities (like “3eyedraven Cyber Club” or departmental initiatives) can enhance peer-based sensitization and improve collective vigilance.

5. Policy Reform and Enforcement:

   Government agencies such as NITDA and NCC should collaborate with tertiary institutions to design national policies mandating minimum cybersecurity awareness standards for all academic institutions.

6. Regular Simulation Exercises:

Conducting simulated phishing attacks and awareness drills at intervals will test student readiness and strengthen individual capacity to detect manipulative attempts.

7. Research and Continuous Improvement:

   Future academic research should explore advanced artificial intelligence models for detecting social engineering attempts in academic emails, portals, and social networks.

8. Based on the findings, a Campus Cyber Complaint Portal was developed as part of this study to provide a structured reporting and response mechanism for social engineering incidents. The system allows students and staff to submit cyber-related complaints in real time, enabling the ICT department to track, verify, and respond to emerging manipulation threats on campus.

5.5 Suggestions for Further Studies

While this study provided useful insights into campus-based social engineering attacks, future studies could explore:

1. Comparative analysis between public and private universities to identify institutional differences in vulnerability.
2. The role of artificial intelligence and machine learning in detecting psychological manipulation patterns in academic networks.

3. Gender-specific susceptibility to social engineering and the impact of digital literacy programs on reducing vulnerability.

5.6 Contribution to Knowledge

This research contributes to the growing body of knowledge in cybersecurity by:

- Demonstrating the unique patterns of social engineering specific to university environments.
- Expanding the understanding of psychological and behavioral dynamics influencing digital vulnerability.
- Providing a policy-oriented framework for academic institutions to build internal cyber resilience.
- Introducing new evidence on peer-based and institutional-level interventions suitable for Nigerian academic settings.

5.7 Concluding Remark

Social engineering continues to evolve as attackers exploit trust, emotion, and curiosity—the most human aspects of interaction. However, through informed awareness, institutional vigilance, and collective responsibility, the university ecosystem can transform from a target zone into a model for national cyber resilience.

This study therefore stands as both a warning and a roadmap for Nigerian campuses seeking to strengthen their defenses against an ever-changing digital threat landscape.

REFERENCES

Adeleke, T., & Sanni, I. (2021). Baiting and removable media attacks in Nigerian university libraries. Journal of Cybersecurity Studies, 9(2), 44–59.

Aguiyi, C., Eze, J., & Nnamdi, O. (2025). Student vulnerability and cyber manipulation in Nigerian tertiary institutions. African Journal of Digital Security, 12(1), 22–34.

Afolabi, M., & Iroko, T. (2022). Digital deception and cyber-awareness among undergraduates. International Journal of Information Security, 18(3), 118–129.

Bada, A., Ezinne, C., & Yusuf, M. (2022). Psychological triggers and cyber-victim susceptibility. Journal of Social Psychology and Technology, 5(1), 55–73.

Badamasi, A., & Utulu, R. (2021). Cyber risk management in Nigerian universities: A conceptual framework. Journal of Information Security Governance, 7(4), 90–103.

Bamidele, O., Hassan, R., & Yusuf, K. (2021). Behavioral analysis of cyber-victims in higher education institutions. Nigerian Journal of Cyber Psychology, 3(2), 64–79.

Bello, L., & Ajao, A. (2024). Curriculum and digital skills development in Nigerian universities. Journal of Digital Education Reform, 6(1), 20–35.

Burgoon, J. (2020). Interpersonal deception theory and communication influence. Oxford University Press.

Cohen, L., & Felson, M. (2020). Routine activity theory and crime environments. Criminology Review, 47(1), 88–103.

Eze, C., & Yusuf, M. (2020). Network vulnerabilities in public universities. Journal of

Cybercrime and Higher Education, 4(2), 25–39.

Gragg, D. (2020). The human element in digital intrusion. Cybersecurity Perspectives, 11(3), 33–48.

Hadnagy, C. (2021). Social engineering: The science of human hacking. HarperCollins.

IBM Security. (2023). Cost of data breach and human error statistics. IBM Press.

Martins, O. (2023). Social media usage and cyber-attack exposure among undergraduates.

Social Computing and Digital Society, 8(1), 51–70.

NITDA. (2021–2024). Digital States and 3MTT Cyber Capacity Development Programme.

National Information Technology Development Agency, Nigeria.

Nwogu, P., & Agbo, J. (2022). Cyber hygiene knowledge among Nigerian university students.

Journal of Information Society Research, 10(4), 77–89.

Nwajioha, C., & Oshim, K. (2025). Social engineering exposure in Ebonyi State University. Journal of Campus Cyber Resilience, 2(1), 14–29.

Ojugo, A., & Otakore, R. (2018). Awareness intervention against phishing attacks in institutions. Computing and Cyber Education Journal, 6(3), 42–58.

Okafor, A., & Adewale, G. (2023). Digital literacy and phishing detection ability among undergraduates. West African Journal of Digital Learning, 9(2), 101–116.

Okokpujie, I., Adedeji, A., & Salami, K. (2025). Psychological manipulation and cyber-fraud activities among students. International Review of Cybercrime Studies, 11(1), 17–30.

Okoye, T., & Alhassan, R. (2022). Campus-based cybercrimes and student data vulnerability.

Journal of ICT and Society, 7(1), 60–73.

Ogundele, R., Ibrahim, S., & Musa, H. (2023). Credential exchange and quid pro quo cyber incidents among youths. African Information Security Journal, 5(2), 29–41.

Shahzad, H., Khanna, A., & Rehman, S. (2022). Social engineering detection using machine learning. Computers & Security, 115, 102–129.

Ugwu, M., Ojo, T., & Eke, A. (2023). Gender and discipline factors in cybersecurity awareness.

Journal of Digital Risk Management, 4(1), 48–63.

UNESCO. (2022). Digital literacy roadmap for Nigeria. UNESCO Publications.

APENDIX

QUESTIONNAIRE

Title: The Role of Social Engineering in Campus-Based Cybercrimes

This questionnaire is designed to collect data for a research project on 'The Role of Social Engineering in Campus-Based Cybercrimes'. The information provided will be used strictly for academic purposes and treated with utmost confidentiality. Please respond as honestly as possible.

SECTION A: DEMOGRAPHIC INFORMATION

1. Gender: ☐ Male ☐ Female

2. Age Range: ☐ 16–20 ☐ 21–25 ☐ 26–30 ☐ 31 and above

3. Level of Study: ☐ 100L ☐ 200L ☐ 300L ☐ 400L ☐ 500L ☐ Postgraduate

4. Faculty: _____

5. Do you use the Internet regularly? ☐ Yes ☐ No

SECTION B: AWARENESS AND KNOWLEDGE OF SOCIAL ENGINEERING

1. I have heard about social engineering before.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

2. I understand what phishing attacks are.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

3. I can identify fake links or websites used in scams.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

4. I have received some form of cybersecurity education or awareness training. ☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

5. I believe social engineering is a serious threat to students and staff on campus.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

SECTION C: EXPERIENCE WITH SOCIAL ENGINEERING ATTACKS

1. I have received suspicious emails or messages requesting personal information. ☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

2. I have clicked on a link that later appeared to be fraudulent.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

3. I know someone who has been a victim of online scams on campus.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

4. I have personally lost data or money due to a social engineering attack. ☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

5. I report suspicious online activities to relevant authorities or university management.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

SECTION D: INSTITUTIONAL MEASURES AND REPORTING CULTURE

1. The university provides cybersecurity awareness programs for students and staff. ☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

2. There are visible cybersecurity policies implemented by the university. ☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

3. The university has a reporting system for online scams or suspicious activities.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

4. Students and staff take cybersecurity warnings seriously.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

5. The institution encourages responsible digital behavior.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

SECTION E: PREVENTIVE ATTITUDE AND PERSONAL PRACTICES

1. I avoid sharing my personal information online.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

2. I verify the authenticity of links before clicking on them.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

3. I regularly change my passwords and keep them private.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

4. I am cautious about the kind of information I post on social media. ☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

5. I use two-factor authentication on my accounts where possible.
☐ Strongly Agree ☐ Agree ☐ Undecided ☐ Disagree ☐ Strongly Disagree

SECTION F: SUGGESTIONS OR RECOMMENDATIONS

1. What steps do you think the university can take to reduce the rate of social engineering attacks on campus?

_____

_____

_____