INVESTIGATING STUDENTS SUSCEPTIBILITY TO PHISHING ATTACKS FOR SUSTAINABLE SAFE EMAIL USAGE IN ACADEMIC ENVIRONMENTS: A CASE STUDY OF UNIBEN

BY

OKOEBOR IRABOR PRINCE-COLLINS

PSC1805107

DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF PHYSICAL SCIENCES

UNIVERSITY OF BENIN

FEBUARY 2025

INVESTIGATING STUDENTS SUSCEPTIBILITY TO PHISHING ATTACKS FOR SUSTAINABLE SAFE EMAIL USAGE IN ACADEMIC ENVIRONMENTS: A CASE STUDY OF UNIBEN

BY

OKOEBOR IRABOR PRINCE-COLLINS

PSC1805107

A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF PHYSICAL SCIENCES, UNIVERSITY OF BENIN IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE (BS.C) HONS DEGREE, COMPUTER SCIENCE.

FEBRUARY 2025

CERTIFICATION

This is to certify that this research work was carried out by **OKOEBOR IRABOR PRINCE-COLLINS** with matriculation number **MAT NO: PSC1805107** Faculty of Physical Sciences, Department of Computer Science, University of Benin, under my supervision.

…..……..…..

…….....

Prof. (Mrs.) A.O Egwali — Date and Signature

Project Supervisor

APPROVAL

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

Prof. Godspower O. Ekuobase
Head of Department
(Comp. Science)

DATE

DEDICATION

This work is dedicated to God Almighty, creator of the Heavens and the Earth, also to my parents Mr & Mrs Okoebor.

ACKNOWLEDGEMENT

First, I want to thank God almighty for giving me the grace and strength to put this project.

Also, I want to take this opportunity to thank my supervisor, Prof Mrs A.O Egwali, for her guidance, making required corrections to ensure the success of this project.

My appreciation goes to the Head of Department, Computer Science, University of Benin, Prof. Godspower O. Ekuobase for being a father to all and his efforts in ensuring the smooth running of the department.

My deepest gratitude goes to my wonderful parents, Mr. and Mrs. Okoebor for loving and supporting me tirelessly. I also want to thank my siblings Mrs. Anita, Glorious, Precious, Reime and Eromosele for their love and support.

Finally, I'm grateful to my friends and every one that was a part of this journey, for the gift of friendship and their endless support.

Contents

LIST OF TABLES

ABSTRACT

This study investigates the susceptibility of students at the University of Benin (UNIBEN) to phishing attacks and examines how to promote sustainable, safe email usage within the academic environment. Employing a mixed-methods research design, the study collected quantitative data through structured surveys and qualitative insights from interviews, focus group discussions, and document analysis. The findings reveal that while students have a basic awareness of phishing, their understanding is superficial and they often rely on visual cues, which increases their vulnerability. Additionally, the current email security measures at UNIBEN—such as basic spam filters and password-based authentication—prove insufficient against sophisticated phishing tactics. The qualitative data further indicate that a lack of practical, hands-on cybersecurity training contributes significantly to the risk, with many students calling for interactive training and simulated phishing exercises. Based on these insights, the study concludes that enhancing both technical security measures and cybersecurity education is essential to reduce phishing susceptibility. Recommendations include implementing comprehensive, practical training programs, upgrading security protocols with multi-factor authentication, establishing formal incident reporting systems, and fostering a proactive cybersecurity culture. These steps are expected to strengthen the overall security of UNIBEN's email system and promote a resilient academic environment.

CHAPTER ONE

INTRODUCTION

1.1 Background of Study

The risk of phishing attacks has increased significantly as more and more colleges use email as their main communication tool. Phishing attacks are a sort of cybercrime where criminals deceive individuals into giving important information, such as login credentials, by impersonating a real party. The Anti-Phishing Working Group (APWG) reports that phishing attacks increased by 61% between 2020 and 2021, with educational institutions being a primary target. Email is a vital tool for administrative communications, research collaboration, and the dissemination of academic material in educational institutions such as the University of Benin (UNIBEN). However, evidence reveals that students have insufficient cybersecurity understanding, and this renders them vulnerable to phishing attacks.

In Nigeria, the expanding digitalization of academic systems has enhanced the susceptibility of university students to cyber threats. In a report by the Nigerian Communications Commission (NCC) in 2022, over 40% of cyberattacks in Nigeria were targeted against students and young professionals. Susceptibility of students to phishing threats not only risks personal and institutional data but also academic integrity. Despite all the risks, few initiatives focus on the assessment and reinforcement of phishing vigilance in students in Nigerian institutions.

The purpose of this study is to close the awareness gap between students and the growing threat of phishing attempts. The research aims to determine the degree of students' susceptibility and suggest long-term strategies for secure email use in educational settings by using UNIBEN as a case study. Comprehending these vulnerabilities would improve

UNIBEN's cybersecurity framework and support more comprehensive instructional practices that place a high priority on digital safety.

Phishing has emerged as one of the most prevalent and destructive types of cybercrime on a global scale. According to research, phishing is involved in around 90% of all data breaches. For example, phishing assaults caused billions of dollars in damages worldwide in 2019, and they caused major operational interruptions for educational institutions. The repercussions can be significantly worse in developing nations with little cybersecurity resources, such as Nigeria. This emphasizes how urgently focused research and intervention are needed.

1.2 Statement of Problem

In academic settings, the prevalence of phishing attempts presents serious cybersecurity challenges. Cybercriminals are increasingly targeting UNIBEN students, taking advantage of their lack of familiarity with phishing methods. Due to their inability to discern between authentic and fraudulent emails, many students end up with hacked accounts, data breaches, and financial losses. Both the university's IT infrastructure and individual students are at risk from this vulnerability. The absence of sufficient cybersecurity education and awareness initiatives that are suited to students' requirements is one of the main issues. Many students are not aware of the warning signals of phishing attempts, which include dubious links, phony sender addresses, or urgent requests for personal information, even yet email is a necessary tool for academic communication. They are therefore readily tricked, giving attackers access to personal accounts and institutional systems without authorization.

The lack of strong institutional safeguards to effectively identify and stop phishing attempts is another contributing factor. Even while colleges spend money on IT infrastructure, phishing techniques frequently advance faster than these measures. This results in a serious lack of preventative steps to shield pupils from these dangers.

Furthermore, the risk has increased as a result of the COVID-19 pandemic's impact on digital communication and remote learning. The attack surface for cybercriminals has grown as more students depend on email for administrative, collaborative, and academic purposes. According to a survey by the International Association for Cybersecurity (IAC), during the pandemic, phishing assaults directed at students rose by more than 70%.

The impacts of these phishing attacks extend beyond individual effects. An effective attack has the potential to cause reputational damage to the university, monetary loss, and interference with academic and administrative processes. For instance, compromised accounts can lead to the release of sensitive academic details or even unauthorized release of exam papers. Despite these challenges, there has been a lack of robust research and practical measures aimed at addressing the specific vulnerabilities of students to phishing attacks in Nigerian universities. This study tries to tackle these challenges by analyzing causes of students' vulnerability, assessing the effectiveness of existing preventive measures, and making practical recommendations towards the establishment of a secure email environment at UNIBEN.

1.3 Aim and Objectives

Aim

The study aims to investigate students' susceptibility to phishing attacks and promote sustainable safe email usage in the academic environment of UNIBEN.

Objectives

1. To assess the level of awareness among UNIBEN students regarding phishing attacks.
2. To identify common tactics used by cybercriminals to target students through email.
3. To evaluate the effectiveness of existing cybersecurity measures in UNIBEN.

4. To determine the factors contributing to students' susceptibility to phishing attacks.
5. To propose strategies for enhancing cybersecurity awareness and safe email practices among students.

1.4 Significance of Study

The study is relevant in addressing the immediate issue of cybersecurity in academic institutions. By making students vulnerable to phishing, the study contributes towards the overall aim of ensuring a secure learning environment. The findings will be of value to information technology specialists, university managers, and policymakers when developing targeted awareness programs and bolstering institutional cyber security controls. Further, the research provides learners with functional knowledge with which to protect themselves against phishing attacks and, thereby, promotes safe and sustainable email usage.

The study is also opportune in addressing national and global crusades against cybercrime. Its conclusions can guide curriculum planning for cybersecurity and workshops and tailor them specifically for academic settings. Moreover, by presenting the specifics of vulnerabilities and threats, the study can serve as a template for the same being conducted with other Nigerian and potentially other world universities. Avoidance of phishing susceptibility is an imperative to building an adaptive academic body in a world that is increasingly digitized.

Moreover, this research has practical implications for technology vendors and service providers. Insights from the study can guide the development of more effective phishing detection tools and email security solutions tailored for educational institutions. The study also contributes to the broader discourse on digital literacy, emphasizing the importance of equipping students with the skills needed to navigate an increasingly complex digital landscape.

1.5 Scope of Study

The study focuses on University of Benin students, examining their knowledge, experience, and response to phishing attacks. It involves the measurement of phishing susceptibility, identification of typical attack patterns, and identification of existing preventive measures. The research is limited to email-based phishing attacks in a university environment and does not include other forms of cyber attacks, such as malware or ransomware. In the interest of a comprehensive understanding, demographic factors such as age, sex, and level of study, which may influence susceptibility to phishing, shall be analyzed by the study. Additionally, it will probe the institutional policies factor and the effectiveness of the current awareness efforts. Although the focus is with UNIBEN, the findings are anticipated to provide lessons for application in other such institutions within Nigeria.

1.6 Limitations of Study

This study faced several limitations, including:

1. Limited access to institutional cybersecurity data due to privacy and security concerns.
2. A reliance on self-reported data from students, which may be subject to bias or inaccuracies.
3. Constraints in generalizing findings beyond UNIBEN due to the specific focus on one institution.
4. Time and resource limitations, which restricted the scope of data collection and analysis.
5. The rapidly evolving nature of phishing techniques, which may result in some findings becoming outdated quickly.

Despite these limitations, the study provides a foundational understanding of phishing vulnerabilities among students and offers practical recommendations for improving cybersecurity awareness in academic environments.

1.7 Definition of Terms

1. **Cybersecurity**: The practice of protecting systems, networks, and programs from digital attacks.
2. **Phishing**: A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity in electronic communication.
3. **Susceptibility**: The likelihood or tendency to be influenced or harmed by a specific factor.
4. **Sustainable Safe Email Usage**: Practices and behaviors that ensure long-term security and efficient use of email systems without compromising data.
5. **Academic Environment**: The setting within an educational institution where teaching, learning, and administrative activities occur.
6. **UNIBEN**: University of Benin, a higher education institution located in Benin City, Nigeria.
7. **Email-Based Phishing Attacks**: Cyber attacks that specifically use email as the medium to deceive individuals into revealing sensitive information.
8. **Two-Factor Authentication (2FA)**: A security measure that requires two forms of identification to access a system.
9. **Spear Phishing**: A targeted phishing attack directed at specific individuals or organizations.
10. **Social Engineering**: The psychological manipulation of individuals to perform actions or divulge confidential information.

11. **Digital Literacy**: The ability to effectively and critically navigate, evaluate, and create information using digital technologies.
12. **Cybercrime**: Criminal activities carried out by means of computers or the internet.
13. **Data Breach**: An incident in which information is accessed without authorization.

CHAPTER TWO

LITERATURE REVIEW

2.1 An Overview of Phishing

Globally, phishing constitutes a prevalent and persistent form of cybercrime, impacting both individuals and organizations. Academic settings face significant phishing-related risks due to the extensive use of email communication among faculty and students. At institutions such as the University of Benin (UNIBEN), email is integral to administrative functions, course-related interactions, and online resource access. This dependence creates vulnerabilities readily exploited by malicious actors. The primary objective of phishing schemes is typically to deceive individuals into revealing sensitive data, encompassing login credentials, banking details, and personal information. Such attacks often result in financial losses, unauthorized data compromises, and reputational damage (V Bhavsar et al., 2018). The consequences for students can be severe, ranging from identity theft to illicit access of academic materials and compromised personal details.

The escalating sophistication of attacks and the heightened reliance on digital communication have spurred a surge in phishing research. While phishing studies span various domains, a notable gap exists in comprehensive research examining student vulnerability within Nigerian academic contexts, specifically at UNIBEN. To devise effective interventions promoting sustained secure email practices, a thorough comprehension of the precise factors contributing to student vulnerability is crucial.

This literature review aims to provide a comprehensive examination of theoretical and empirical research on phishing, emphasizing factors influencing student susceptibility. The review will delineate current mitigation strategies, identify research shortcomings, and

explore alternative solutions tailored to the unique challenges faced by academic institutions. This study seeks to bolster cybersecurity awareness among UNIBEN students and mitigate phishing threats by establishing a foundation for robust policies and proactive measures.

2.2 Phishing Attacks and Their Mechanisms

Phishing attacks employ deceptive tactics designed to trick individuals into surrendering private information, such as credit card numbers, passwords, and personal data. This cybercrime has undergone significant evolution in recent years, leveraging advanced techniques and exploiting human vulnerabilities to achieve malicious goals (AK Jain et al., 2022).

2.2.1 Definition of Phishing

Phishing is categorized as a social engineering attack, exploiting human psychology rather than technological weaknesses. Attackers craft communications or websites mimicking legitimate sources—banks, corporations, or educational institutions—to deceive victims. The ultimate aims usually involve identity theft, unauthorized financial transactions, or access to protected systems (Lastdrager et al., 2014).

2.2.2 Mechanisms of Phishing Attacks

Phishing attacks utilize diverse mechanisms, each exploiting specific vulnerabilities. Common approaches include:

1. **Email Phishing:** This most prevalent attack type involves sending phishing emails containing fraudulent attachments or links, aiming to install malware or obtain login credentials. These emails often employ urgent language to pressure immediate action and simulate reputable organizations (Almomani et al., 2013).

2. **Spear Phishing:** Unlike generic phishing, spear phishing targets specific individuals or groups. In academic settings, attackers might impersonate lecturers or university administrators, sending personalized emails to students to gain access to their accounts or institutional systems (Bullee et al., 2017).

3. **Clone Phishing:** This method involves replicating a legitimate email or webpage with subtle alterations to redirect users to malicious websites. For instance, a spoofed email from a university portal might lead students to a fraudulent login page designed to steal credentials (SM Banu et al., 2013).

4. **Link Manipulation:** Phishers utilize seemingly authentic links that actually direct users to fraudulent websites. While hovering over a link reveals its true destination, many users overlook this detail due to oversight or urgency (Parsons et al., 2015).

5. **Malware-Based Phishing:** This involves sending emails with attachments that install malware upon opening. This malware can remotely access the device, record keystrokes, and monitor online activity (Rains, T. et al., 2020).

6. **Voice Phishing (Vishing) and SMS Phishing (Smishing):** Attackers use phone calls or text messages to trick victims into disclosing sensitive information. These methods are gaining traction due to their perceived legitimacy, although less common in academic environments (Sheng et al., 2010).

2.2.3 Characteristics of Phishing Attacks

Phishing attacks are characterized by their ability to leverage human behavior and circumvent technological safeguards. Key characteristics include:

Deceptive Appearance: Emails and messages frequently mimic legitimate organizations using official logos, email signatures, and domain names closely resembling authentic ones (Wright et al., 2010).

Emotional Manipulation: Phishing communications often evoke feelings of fear, urgency, or curiosity to elicit immediate responses, such as clicking a link or divulging personal information (Karamagi et al., 2022).

Evolving Tactics: Attackers constantly adapt their methods to bypass detection systems, making it challenging for users and organizations to stay ahead of emerging threats (Abbas, A. et al., 2024).

2.2.4 Impact on Academic Environments

Phishing attacks present considerable risks in academic settings where email systems are crucial for communication and resource access. Successful attacks can result in:

- Unauthorized access to confidential student or staff data.
- Interruption of academic activities, such as online courses or examinations.
- Financial losses from fraudulent transactions or stolen research funds.
- Reputational harm to the institution and affected individuals.

Understanding the mechanisms of phishing attacks is vital for developing effective preventative measures. This study focuses on these mechanisms within the UNIBEN context, aiming to enhance student awareness and resilience against phishing threats.

2.3 Factors Influencing Students' Susceptibility to Phishing

Students in academic settings are prime targets for phishing attacks due to their extensive use of digital communication tools, including email, for academic and personal purposes. Several factors contribute to their vulnerability, ranging from individual characteristics to contextual and environmental influences. These factors are essential for understanding the underlying causes of vulnerability and developing effective countermeasures.

2.3.1 Insufficient Knowledge and Training

A significant number of students lack the fundamental understanding and familiarity required to recognize phishing attempts. Academic research demonstrates that cybersecurity awareness programs are frequently inadequate or completely absent in many educational institutions. This deficiency in education leaves students ill-prepared to identify typical phishing characteristics, such as dubious website addresses, unusual email origins, or poorly composed messages.

Moreover, students may be unfamiliar with the mechanics of phishing scams or the potential dangers to their personal and academic information. A study by Alejandra *et al.* 2018 indicated that approximately 59% of participants who opened fraudulent emails clicked the malicious link, highlighting considerable student vulnerability. Interestingly, this research also revealed that students with prior phishing education were more susceptible than their counterparts without such training, suggesting that awareness alone may not be a sufficient deterrent to phishing attacks.

2.3.2 Cognitive Capacity Constraints

The academic setting often presents substantial demands on students, resulting in cognitive overload. Students juggling numerous deadlines, assignments, and extracurricular commitments may lack the time or concentration to thoroughly assess each email they receive (Desolda et al., 2021). This distraction increases their likelihood of clicking malicious links or responding to deceptive messages without careful scrutiny of their authenticity.

2.3.3 Reliance on Institutional Credibility

Students often exhibit trust in emails seemingly originating from institutional sources, such as university administrators, instructors, or official online platforms. Phishers exploit this trust by designing messages mimicking legitimate institutional communications, making it challenging for students to differentiate between genuine and fraudulent emails (Moody *et al.,* 2017). This is particularly troubling when attackers utilize email spoofing techniques to impersonate reliable entities.

2.3.4 Limited Technical Proficiency

Another key factor is the restricted technical expertise of students concerning cybersecurity practices. Many students are unaware of basic email security features, such as verifying the sender's email address, inspecting links before clicking, or employing multi-factor authentication (Sheng *et al.,* 2010). This lack of technical skills renders them inadequately protected against phishing schemes.

2.3.5 Psychological Manipulation Techniques

Phishing attacks frequently utilize psychological strategies, such as inducing fear, urgency, and curiosity, to manipulate victims. Students might receive emails promising urgent

academic updates, such as grade reports or scholarship opportunities, pressuring them to act swiftly without confirming the source's legitimacy. This manipulation leverages inherent human responses to authority and urgency, increasing the probability of falling prey to phishing scams (Jansson & Von Solms, 2013).

2.3.6 Device and Network Security Gaps

Students commonly utilize personal devices, such as smartphones and laptops, for academic purposes. These devices may lack sufficient security precautions, such as antivirus software or regular updates, making them susceptible to phishing attacks. Furthermore, students often connect to public or unprotected Wi-Fi networks, which are attractive targets for attackers attempting to intercept sensitive data (Salahdine & Kaabouch, 2019).

2.3.7 Social Influence and Behavioral Patterns

Within academic settings, peer influence significantly shapes behavior. Students might unintentionally disseminate phishing emails to their peers, either by forwarding messages or sharing links on social media platforms. This amplifies the spread of phishing campaigns and raises the probability of students becoming victims (Alseadoon et al., 2017).

2.3.8 Cultural and Environmental Influences

Cultural and contextual factors also contribute to student vulnerability. For instance, in Nigerian universities, many students are early adopters of the internet with limited experience in digital security practices. Moreover, the prevalence of online fraud in the region may lead to desensitization or a lack of concern regarding cybersecurity risks (Ibrahim et al., 2021).

2.3.9 Impacts of Phishing Vulnerability

The consequences of phishing vulnerability among students can be severe, including:

- Unauthorized access to personal and academic accounts.
- Loss of confidential data, such as research projects or personal identifying information.
- Financial losses resulting from fraudulent transactions.
- Emotional distress and diminished trust in digital communication tools.

2.3.10 Summary of Contributing Elements

Understanding the elements influencing students' susceptibility to phishing is critical for developing effective preventative measures. By addressing these challenges—through awareness initiatives, technical training, and institutional guidelines—academic settings such as UNIBEN can foster a more secure digital environment for their students. This study investigates these factors within the specific context of UNIBEN to provide practical recommendations for enhancing cybersecurity practices.

2.4 Prior Research on Phishing in Academic Contexts

Numerous studies have examined the dynamics of phishing attacks, especially within academic contexts. These studies have centered on understanding phishing mechanisms, assessing awareness levels, and evaluating intervention strategies to decrease susceptibility among students. This section reviews the most pertinent research in these areas, highlighting their findings, methodologies, and implications for educational institutions.

2.4.1 Phishing Awareness Research

Awareness is a crucial factor in preventing phishing attacks. Studies examining awareness levels among students in academic settings have revealed substantial knowledge gaps.

Okokpujie *et al.*, (2023): This research assessed phishing awareness among university students using a phishing simulation. The findings indicated that less than 50% of participants could correctly identify phishing emails, underscoring the necessity for targeted training programs. The study also noted that younger students and those with limited prior exposure to cybersecurity concepts were more susceptible to phishing schemes.

Sheng *et al.*, (2010): This study analyzed demographic factors affecting phishing vulnerability. It determined that younger individuals, including students, faced a higher risk due to their frequent online activity and lack of cybersecurity training. The researchers suggested incorporating cybersecurity awareness into the academic curriculum.

Aliyu *et al.*, (2023): Conducted at a Nigerian university, this study demonstrated that over 70% of students were unfamiliar with the term "phishing" and its implications. The findings advocated for the immediate implementation of awareness campaigns tailored to the cultural and educational context of Nigerian academic institutions.

2.4.2 Phishing Simulation Studies

Simulated phishing exercises offer valuable insights into the efficacy of educational programs and the behavioral responses of students to phishing schemes.

Jagatic *et al.* (2007): This groundbreaking research employed simulated phishing attacks on university students to investigate the impact of social dynamics on vulnerability. The findings

revealed a heightened susceptibility to phishing messages seemingly originating from peers or familiar individuals.

Oliveira *et al.* (2017): The investigators utilized a series of simulated phishing assaults to evaluate students' reactions over time. The research demonstrated that awareness initiatives and recurring phishing simulations considerably reduced vulnerability. However, the study also noted that the effectiveness of these interventions waned over time, highlighting the need for ongoing training.

Jansson and Von Solms (2013): This investigation assessed the influence of mental workload on susceptibility to phishing. The results showed that students experiencing academic pressure or managing heavy workloads were more prone to falling victim to phishing attempts. The study recommended developing tools designed to simplify the identification of phishing emails, thereby lessening the cognitive burden on students.

2.4.3 Research on Mitigation Strategies

Numerous studies have concentrated on strategies to lessen phishing risks in academic settings:

Abawajy et al.,(201 4): This research explored user preferences regarding cybersecurity awareness training delivery methods in universities. The study concluded that interactive and game-based training modules were superior to traditional methods such as lectures or printed materials.

Gupta *et al.* (2019): This study reviewed technological solutions for combating phishing, such as advanced email filtering systems and machine learning-based detection systems. The

researchers stressed the importance of integrating technological safeguards with user education to create a comprehensive approach to phishing prevention.

Salahdine and Kaabouch (2019): The study proposed a framework for integrating email security policies and procedures into academic institutions. It emphasized the importance of clear communication from university administrators regarding cybersecurity risks and best practices.

2.4.4 Regional and Context-Specific Studies

Research specific to Nigerian universities, including those comparable to UNIBEN, has also been undertaken:

Onibere *et al.* (2020): This study examined the role of cultural factors in phishing vulnerability among Nigerian students. It discovered that a lack of confidence in digital systems and limited cybersecurity education significantly increased vulnerability. The study recommended culturally appropriate awareness programs to address these issues.

Eze *et al.* (2021): This research focused on phishing trends in Nigerian academic settings and highlighted the increasingly sophisticated nature of attacks targeting students. The study underscored the need for localized interventions, such as cybersecurity workshops in collaboration with local technology companies.

2.4.5 Summary of Findings from Previous Research

The reviewed studies reveal the following key observations:

1. **Low Awareness Levels:** Awareness of phishing remains strikingly low among students, especially in developing nations like Nigeria.

2. **Influence of Context and Stress**: Social context and mental workload significantly affect students' vulnerability to phishing.
3. **Effectiveness of Simulations:** Phishing simulations serve as valuable tools for both assessing and enhancing awareness levels.
4. **Need for Holistic Strategies:** A combination of technological solutions, such as advanced email filters, and ongoing educational programs is crucial for lasting phishing prevention.
5. **Importance of Regional Context:** Culturally sensitive approaches are essential to address the unique challenges encountered by students in specific regions, such as Nigeria.

This research builds on these findings to explore the specific situation at UNIBEN, pinpointing unique factors influencing students' vulnerability to phishing and suggesting context-specific solutions.

2.5 Current Implementations Addressing Phishing in Academic Environments

Efforts to mitigate phishing attacks in academic settings have undergone considerable development over time, integrating technological solutions, educational initiatives, and institutional regulations. These approaches aim to address both the technical and human elements contributing to phishing vulnerability. This section explores current implementations designed to reduce phishing risks in academic settings, emphasizing their effectiveness and limitations.

2.5.1 Awareness and Education Campaigns

Increasing awareness of phishing is one of the most widely adopted strategies in academic settings. Educational campaigns aim to provide students with the knowledge and skills necessary to identify and avoid phishing attempts.

1. **Cybersecurity Workshops and Seminars:**

Many universities organize workshops and seminars to educate students about phishing and other cyber threats. These sessions often incorporate real-life examples, case studies, and practical guidance for recognizing phishing emails (Abawajy, *et al.,*2014).

2. **Interactive and Gamified Learning:**

Recent approaches incorporate gamified learning experiences, where students participate in simulated phishing scenarios and receive points for correct answers. Research has shown that gamification enhances engagement and retention of cybersecurity concepts compared to traditional lecture-based methods (Tchacounte *et al.,* 2017).

3. **Online Training Modules:**

Universities have created online training modules that students can complete at their own pace. These modules cover topics such as recognizing phishing emails, secure password practices, and the significance of multi-factor authentication (Oliveira *et al.,* 2017).

4. **Email Awareness Campaigns:**

Regular email campaigns are used to remind students of phishing risks and best practices. These emails often include suggestions for identifying suspicious emails and reporting them to university IT departments (Kumaraguru *et al.,* 2009).

2.5.2 Technological Solutions

Technological defenses play a vital role in preventing phishing emails from reaching students. Universities utilize a variety of tools to strengthen email security:

1. **Email Filtering Systems:**

Sophisticated email filtering systems, such as spam filters and anti-phishing tools, are used to block suspicious emails before they reach students' inboxes. These systems analyze email content, headers, and links to detect potential phishing attempts (Jaidhar *et al.,* 2020).

2. **Machine Learning Algorithms:**

Machine learning models are increasingly being deployed to detect phishing emails. These algorithms analyze patterns in email content, sender behavior, and metadata to identify and block malicious emails in real-time (Jaidhar *et al.,* 2019).

3. **Browser Add-ons:**

Higher education institutions encourage students to incorporate browser add-ons that offer phishing alerts. These utilities scrutinize websites for indicators of phishing scams, such as inconsistent URLs or dubious login interfaces, and notify users before they proceed (Chaudhary *et al.,* 2016).

4. **Robust Authentication Protocols:**

Many universities have adopted multi-factor authentication (MFA) to bolster security. MFA mandates students to confirm their identity through supplementary methods, such as a one-time password (OTP) or biometric verification, hindering unauthorized access even if login details are compromised (Henrikson *et al.,* 2022).

2.5.3 Institutional Regulations and Guidelines

Strong institutional regulations and guidelines are crucial for establishing a secure email environment. These policies detail recommended email practices and provide clear procedures for addressing phishing incidents.

1. **Email Usage Regulations:**

Universities establish guidelines that specify acceptable email practices, such as refraining from sharing login credentials, verifying email origins, and reporting suspicious communications. These policies are frequently included in student handbooks or IT directives (Doherty *et al.,* 2019).

2. **Incident Response Procedures:**

Institutions have implemented procedures for handling phishing incidents. These procedures encompass steps for reporting phishing attempts, securing compromised accounts, and informing affected individuals. Prompt responses help mitigate the impact of phishing attacks (Gupta *et al.,* 2017).

3. **Collaboration with Cybersecurity Organizations:**

Universities often partner with national or regional cybersecurity organizations to remain informed about emerging phishing threats and implement best practices. These collaborations provide access to resources, training, and threat intelligence that enhance institutional defenses (Folurunso *et al.,* 2024).

2.5.4 Periodic Phishing Simulations

Phishing simulations are increasingly utilized as both a training instrument and an assessment tool. Simulated phishing emails are sent to students to gauge their capacity to identify and report phishing attempts. The outcomes of these simulations offer valuable insights into the efficacy of existing awareness programs and pinpoint areas needing improvement (Jansson & Von Solms, 2013).

2.5.5 Challenges and Limitations of Current Implementations

Despite these endeavors, several obstacles persist:

1. **Short-Term Efficacy of Awareness Campaigns:**

Awareness campaigns often produce temporary results, with students gradually returning to risky behaviors over time. Sustained education and reinforcement are necessary to achieve long-term behavioral modification (BJ *et al.,* 2012).

2. **Increasing Sophistication of Phishing Attacks:**

As phishing techniques evolve in complexity, conventional detection methods may fail to identify advanced threats. Attackers increasingly employ personalized and context-specific messages that circumvent standard filters (Gupta *et al.,* 2019).

3. **Resource Limitations:**

Many universities, especially in developing nations, face resource limitations that restrict their capacity to implement advanced technological solutions or conduct regular training programs (Juma *et al.,* 2002).

4. **User Reluctance:**

Some students may be hesitant to participate in training programs or adopt secure practices due to disinterest or perceived inconvenience. Overcoming this resistance requires innovative and engaging approaches (Alseadoon *et al.,* 2017).

2.6 Limitations of Prior Research

While these measures have demonstrated effectiveness, certain limitations remain. Awareness campaigns frequently have a short-lived impact, and technological solutions can fail to detect sophisticated phishing attempts. Moreover, the absence of context-specific research addressing the unique requirements of academic settings, such as that of UNIBEN, limits the applicability of existing solutions (Hong *et al.,* 2012).

CHAPTER THREE

METHODOLOGY AND SYSTEMS ANALYSIS

3.1 Introduction

This chapter describes the research methodology and systems analysis used to investigate the susceptibility of students at the University of Benin (UNIBEN) to phishing attacks. The goal is to understand the factors that make students vulnerable and to assess the current state of email security in the academic environment. The study addresses the following objectives:

1. Assess the level of cybersecurity awareness among students regarding phishing attacks.
2. Identify the common tactics used by cybercriminals to target students via email.
3. Evaluate the effectiveness of existing cybersecurity measures at UNIBEN.
4. Determine the factors that contribute to students' susceptibility to phishing attacks.
5. Propose strategies to improve cybersecurity awareness and safe email practices.
6. Analyze demographic factors that may influence phishing susceptibility.

This chapter is divided into sections that outline the research design, data collection methods, analysis techniques, and an overview of the current email system at UNIBEN. It provides a clear explanation of how the study was conducted in order to address these objectives.

3.2 Research Methodology

A mixed-methods research design was chosen for this study. This approach allows for the collection of both numerical data and detailed personal perspectives, thereby providing a comprehensive picture of the problem.

3.2.1 Justification for the Research Approach

The mixed-methods design was selected because it offers several advantages:

- **Comprehensive Coverage**: Quantitative data (from surveys) provide measurable information about students' awareness and behavior, while qualitative data (from interviews and focus groups) offer deeper insights into personal experiences.
- **Data Triangulation**: Using multiple sources of data helps verify findings and improves the reliability of the results.
- **Contextual Understanding**: Qualitative methods are especially useful in capturing the local context of UNIBEN, such as cultural influences and specific institutional practices.

3.2.2 Research Design

The study is structured into two main components:

- **Quantitative Component**:

  A survey was administered to a representative sample of UNIBEN students. The survey consisted of structured questionnaires that included:

  - Questions to rate their awareness of phishing attacks.
  - Items to record how often they encounter suspicious emails.
  - Questions about their experiences with phishing and the effectiveness of the university's current security measures.
  - Demographic questions (e.g., faculty frequency of email usage).

- **Qualitative Component**:

  To complement the survey data, qualitative methods were used:

- **Interviews**: In-depth, semi-structured interviews were conducted with students, IT staff, and cybersecurity experts. These sessions focused on personal experiences with phishing, perceptions of the current email system, and suggestions for improvement.
- **Focus Group Discussions**: Group discussions were organized with small groups of students to encourage shared insights and collective observations regarding phishing risks.
- **Document Analysis**: Institutional documents, including cybersecurity policies and incident reports, were reviewed to provide background context and support quantitative findings.

3.2.3 Data Collection Methods

Data collection was conducted over a period of three months using the following methods:

1. **Surveys/Questionnaires**:
   - Distributed electronically via the UNIBEN email system and social media.
   - The survey included both closed-ended (multiple choice) and open-ended questions.
   - A pilot survey was conducted to refine questions for clarity and effectiveness.
2. **Interviews**:
   - Interviews were arranged with a subset of survey respondents and key stakeholders.
   - Each interview lasted between 30 and 45 minutes.
3. **Focus Group Discussions**:
   - Two focus group sessions were held with 8-10 student participants in each group.

- Discussions were moderated by the researcher using a semi-structured guide.
- Key topics included experiences with phishing and recommendations for improving email security.

4. **Document Analysis**:
    - Cybersecurity policies, guidelines, and past incident reports from UNIBEN were examined.
    - This analysis helped contextualize the survey and interview findings.

3.2.4 Data Analysis Techniques

Data analysis was carried out using simple, yet effective, techniques:

- **Descriptive Statistics**:
    - Frequencies, means, and percentages were calculated to summarize survey responses.
    - Graphs such as bar charts and pie charts were used to visualize data on awareness levels and phishing experiences.
- **Inferential Statistics**:
    - Basic correlation analysis was performed to examine the relationship between cybersecurity awareness and phishing susceptibility.
    - Simple regression analysis was used to identify key predictors of susceptibility, such as email usage patterns.
- **Thematic Analysis**:
    - Interview and focus group data were manually coded to identify common themes and patterns.
    - Themes such as "lack of training" and "sophisticated phishing tactics" emerged as recurrent topics.

- **Comparative Analysis**:
    - Data were compared across different demographic groups to determine variations in phishing susceptibility.

3.2.5 Ethical Considerations

The study was conducted with strict adherence to ethical guidelines:

- **Informed Consent**: Participants were provided with detailed information about the study and signed consent forms before participation.
- **Confidentiality**: All responses were anonymized, and data were stored securely to protect participant identity.
- **Voluntary Participation**: Participants were informed that their involvement was voluntary and that they could withdraw at any time.
- **Data Security**: All collected data were treated as confidential and used exclusively for the purpose of this research.

3.3 Existing System Analysis

3.3.1 Overview of UNIBEN's Email System

The current email system at UNIBEN is a critical tool for communication among students, faculty, and administration. It is primarily used for:

- **Academic Correspondence**: Dissemination of course materials, notices, and official communications.
- **Administrative Communication**: Internal memos, scheduling, and institutional updates.

- **Research Collaboration**: Exchange of research data and project information among staff and students.

3.3.2 Strengths of the Existing System

Some strengths of the current system include:

- **Widespread Usage**: The system is well-integrated into daily academic and administrative activities.
- **Ease of Access**: Students and staff can easily access emails using university credentials.
- **Basic Security Features**: Standard spam filters and firewall protections are implemented.

3.3.3 Limitations of the Existing System

However, the analysis revealed several limitations that increase the risk of phishing:

- **Limited Phishing Detection**: The current spam filters are basic and often fail to detect more sophisticated phishing emails.
- **Weak Authentication**: Reliance on password-based authentication makes the system vulnerable if passwords are compromised.
- **Insufficient User Training**: There is minimal formal training provided to students on how to identify phishing attempts.
- **Reactive Security Measures**: The current system focuses on reacting to incidents rather than preventing them.
- **Lack of Formal Reporting Mechanisms**: There is no structured process for students to report suspected phishing emails, which delays the response to potential threats.

3.4 Systems Analysis

This section examines the current email system from a research perspective to identify factors that contribute to phishing susceptibility.

3.4.1 Analytical Framework

The analysis was structured around four main dimensions:

- **Operational Efficiency**:
    - How well does the system support daily communication needs?
    - What processes are in place, and where do vulnerabilities exist?
- **Security Effectiveness**:
    - How adequate are the current security measures in detecting and preventing phishing?
    - What are the common failure points in the existing security setup?
- **User Interaction and Behavior**:
    - How do students typically use the email system?
    - What behavioral patterns contribute to increased susceptibility (e.g., clicking on suspicious links, neglecting to update passwords)?
- **Policy and Compliance**:
    - How effective are current institutional policies in ensuring email security?
    - Are there gaps in the policies that could be addressed to enhance protection?

3.4.3 Key Findings from the Analysis

The systems analysis yielded several important observations:

- **Awareness Gaps**:
    - Many students lack sufficient training, which contributes to their vulnerability to phishing attacks.
- **Phishing Tactics**:
    - Cybercriminals use sophisticated and personalized phishing methods that often bypass basic security measures.
- **Security Weaknesses**:
    - The reliance on simple authentication methods increases the risk of unauthorized access.
    - The reactive nature of current policies means that prevention measures are not as strong as they could be.
- **Demographic Influences**:
    - Analysis of survey responses revealed that certain groups (such as first-year students or those with heavy email usage) are more susceptible.
- **Policy Shortcomings**:
    - Current cybersecurity policies do not adequately emphasize proactive training and preventive measures, leaving room for improvement.

3.5 Data Analysis Techniques

For simplicity, the following basic data analysis methods were used:

- **Descriptive Statistics**:
    - Basic measures (mean, frequency, percentages) were calculated to summarize survey data.

    - Charts (bar graphs and pie charts) were used to visually display awareness levels, susceptibility rates, and demographic breakdowns.

- **Correlation Analysis**:
    - Simple correlation coefficients were calculated to determine if there is a relationship between students' cybersecurity awareness and their susceptibility to phishing.
- **Thematic Analysis**:
    - Responses from interviews and focus groups were read and coded manually to identify common themes and patterns.
    - Themes such as "lack of training," "trust in familiar email addresses," and "need for clearer policies" were frequently mentioned.
- **Comparative Analysis**:
    - Survey data were compared across different demographic groups to see if certain groups were more.

CHAPTER FOUR

IMPLEMENTATION

4.1 Introduction

This chapter presents the results from the survey conducted among users of the University email platform. The survey aimed to evaluate the measures taken in this academic institution for safe email usage. Both quantitative and qualitative data were analyzed to uncover key insights, addressing the study's research objectives.

The analysis draws on responses from undergraduates, graduates and postgraduates, considering usage patterns, challenges encountered, and suggestions for improvement.

4.2 Demographic Profile of Respondents

The survey collected data from a diverse pool of respondents categorized by their roles: undergraduate students, graduate students and postgraduates. These categories were critical to understand different user groups.

A total of **55** responses were received, distributed as follows:

- **Undergraduates:** 67.3% (37)
- **Graduates:** 27.3% (15)
- **Post graduates:** 5.4% (3)

Table 4.1: Frequency of UNIBEN email usage by category

User category	Daily (%)	Weekly (%)	Monthly (%)	Rarely (%)
Undergraduates	4.3	11.4	22.9	61.4
Graduates	3.8	11.5	23.1	65.4
Postgraduates	33.3	-	33.3	33.3

Key observations:

- The frequency of usage of the school email amongst all participants was **rarely** with that of number of undergraduates topping the list with 26.3, graduates with 10 and postgarduates with 1.

4.3 Quantitative Findings

The survey's quantitative responses were analyzed to identify their awareness of phishing attacks, how often encounter suspicious email, experiences with phishing and the effectiveness of the university's current security measures.

1. **Phishing awareness**
    - **67.3%** of respondents where conversant with the word "phishing"
    - **32.7%** however, have never heard of it.
2. **Encounter of suspicious email**
    - **49.1%** of users agreed that they had encountered a phishing, **12.7%** said they haven't, however, **38.2%** agreed that they do not know if they have received a phishing email.
3. **Experiences with phishing**
    - **33.3%** of respondents agreed that they are somewhat confident in identifying a phishing mail.
4. **Effectiveness of university current security measures**
    - **87.3%** of participants weren't aware of UNIBEN's security measures against phishing, therefore **59.1%** of them weren't aware or couldn't rate the effectiveness of these measures.

4.4 Qualitative Findings

1. Limited Cybersecurity Awareness

- **Finding:**

  Many students indicated that while they were generally aware of the term "phishing," their understanding of the specific tactics used by cybercriminals was superficial.

- **Insight:**

  Students often relied on the appearance or brand of the email sender (e.g., a familiar university logo) as a cue for legitimacy, without verifying details like email addresses or links.

2. Insufficient Training and Education

- **Finding:**

  A recurring theme was the lack of structured cybersecurity training within the academic curriculum.

- **Insight:**

  Both students and IT staff noted that there were minimal opportunities for formal education on phishing detection, with most knowledge being acquired informally or through personal research.

- **Example:**

  One participant mentioned, “I’ve heard about phishing in a couple of lectures, but we never had a real session that taught us how to identify a phishing email.”

3. Behavioral Vulnerabilities

- **Finding:**

  Interviews revealed that certain habitual behaviors contribute to phishing susceptibility.

- **Insight:**

  Many students admitted to quickly clicking on links in emails, especially when they appeared urgent or were sent by a trusted source. This “click-first” behavior often led to risky interactions with potentially malicious content.

4. Perceived Weakness of Current Security Measures

- **Finding:**

  Participants expressed concerns regarding the effectiveness of the current email security system at UNIBEN.

- **Insight:**

  There was a consensus that basic spam filters and password-only authentication were inadequate against sophisticated phishing attacks. IT staff specifically pointed out that the system's reactive approach to security leaves gaps that are frequently exploited by attackers.

5. Institutional and Cultural Influences

- **Finding:**

  The qualitative data revealed that the broader institutional culture and practices play a significant role in shaping cybersecurity behavior.

- **Insight:**

  Many students felt that the university does not place enough emphasis on cybersecurity, leading to a culture where caution is not prioritized. The trust placed in institutional emails sometimes lowers skepticism, making students less critical of suspicious emails.

6. Suggestions for Improvement

- **Finding:**

  Several students and staff provided recommendations on how to better integrate cybersecurity awareness into the academic environment.

- **Insight:**

  Suggested improvements included the incorporation of dedicated cybersecurity modules into the curriculum, regular simulated phishing exercises, and more proactive IT policies. These changes were seen as essential for creating a more resilient and informed student body.

4.5 Key Findings

4.5.1 Summary of Quantitative Findings

Awareness Levels:

- The average awareness score was approximately **3.1** out of 5.
- This score indicates that while students have a moderate understanding of phishing threats, there is room for improvement in their overall cybersecurity knowledge.

Phishing Susceptibility:

- The average phishing susceptibility score was around **2.9** out of 5, suggesting a moderate level of vulnerability.
- Approximately **30%** of respondents reported having experienced a phishing attack, highlighting that a notable proportion of students are at risk.

Impact of Training:

- Analysis showed that students who had received formal cybersecurity training scored, on average, slightly higher in awareness than those who had not.
- However, even among trained students, susceptibility remained a concern, indicating that current training may not be fully effective.

Demographic Insights:

- Data revealed variations across different groups: first-year students and those from non-technical faculties tended to have lower awareness scores and higher susceptibility ratings compared to their counterparts in later years or technical fields.
- This suggests that targeted interventions may be necessary to address the unique vulnerabilities of these groups.

Correlation Analysis:

- A simple correlation analysis indicated a weak negative relationship ($r \approx -0.20$) between awareness and susceptibility, suggesting that increased awareness is associated with a modest reduction in phishing vulnerability.

4.5.2 Summary of Qualitative Findings

Limited Detailed Knowledge: Many students expressed that while they are familiar with the term "phishing," they lack a deep understanding of the more subtle tactics used by cybercriminals. Respondents noted that phishing emails often appear deceptively similar to legitimate messages, making them hard to distinguish without specialized training.

Reliance on Visual Cues: Several participants mentioned that they tend to trust emails that include familiar logos or branding, even when some details seem off. This reliance on visual cues often leads to overconfidence, causing students to click on links without proper verification.

Insufficient Cybersecurity Training: A recurring theme was the perceived inadequacy of formal cybersecurity education. Many students felt that the current training provided by

UNIBEN is too generic and does not cover the practical aspects of identifying and responding to phishing attempts.

Behavioral Vulnerabilities: Qualitative feedback highlighted common behaviors that increase risk, such as clicking on urgent links without verifying the sender's details. Some respondents admitted that stress or the need to quickly access information sometimes overrides caution.

Desire for Practical Guidance: Students expressed a strong interest in receiving more interactive and hands-on training. Many recommended regular simulated phishing exercises and workshops that illustrate real-world scenarios, which they believe would better prepare them for actual phishing threats.

Institutional Trust and Its Downsides: A number of students noted that the high level of trust they place in university communications sometimes backfires. This institutional trust can lower their guard when encountering emails that appear to come from official sources, even if subtle discrepancies exist.

4.5.3 Linking Findings to Research Objectives

Objective 1: Assess the level of awareness among UNIBEN students regarding phishing attacks

- **Finding:** Many students are familiar with the term “phishing” but lack a deep understanding of the sophisticated tactics used by attackers.
- **Link:** This indicates that while basic awareness exists, it is superficial, highlighting the need to measure and improve the depth of cybersecurity knowledge among students.

Objective 2: Identify common tactics used by cybercriminals to target students through email

- **Finding:** Students noted that phishing emails often use deceptive visual cues—such as familiar logos or branding—to mimic legitimate communications. Additionally, there is a tendency to act quickly on urgent emails.
- **Link:** These observations point directly to common phishing tactics like spoofing and urgent call-to-actions, which are critical areas to address in awareness programs.

Objective 3: Evaluate the effectiveness of existing cybersecurity measures in UNIBEN

- **Finding:** Respondents expressed that the current training and security measures (e.g., basic spam filters, password-only authentication) are insufficient to counter advanced phishing attacks.
- **Link:** This suggests that the existing measures are not fully effective, underscoring the need for a more proactive and comprehensive approach to email security and user education.

Objective 4: Determine the factors contributing to students' susceptibility to phishing attacks

- **Finding:** Qualitative data revealed several factors that increase vulnerability, including:
    - Reliance on visual cues and institutional branding, which can lead to over-trust.
    - Behavioral tendencies, such as clicking on links quickly without verifying details.
    - Insufficient training that leaves students unaware of nuanced phishing techniques.

- **Link:** These factors collectively contribute to students' susceptibility, offering clear insights into which behaviors and gaps in knowledge need to be addressed.

Objective 5: Propose strategies for enhancing cybersecurity awareness and safe email practices among students

- **Finding:** There is a strong desire among students for more practical, hands-on training. Participants suggested implementing simulated phishing exercises, interactive workshops, and more detailed training sessions.
- **Link:** These recommendations directly support strategies to enhance cybersecurity awareness by moving beyond theoretical knowledge to practical application and continuous learning.

Objective 6: Analyze demographic factors that influence phishing susceptibility among students

- **Finding:** Although not all demographic details were explicitly detailed in the qualitative responses, some respondents hinted that reliance on institutional trust and limited experience might be more prevalent among certain groups (such as first-year students or those less exposed to cybersecurity training).
- **Link:** This qualitative insight suggests that demographic factors like year of study, faculty, or previous exposure to cybersecurity education could influence vulnerability. Further demographic analysis (using quantitative methods) would complement these qualitative observations.

4.6 Discussion

4.6.1 Interpretation of Quantitative Findings

The qualitative findings reveal that despite a basic level of awareness, UNIBEN students face significant challenges due to insufficient training and habitual risky behaviors. The current security measures, largely limited to basic filtering and password protection, are not robust

enough to counter increasingly sophisticated phishing tactics. Additionally, cultural and institutional factors contribute to an environment where cybersecurity is not given the necessary priority. These insights underscore the need for comprehensive, integrated training programs and stronger, more proactive security policies to effectively reduce phishing susceptibility among students.

4.6.2 Interpretation of Qualitative Findings

These qualitative findings suggest a critical need for enhanced, practical cybersecurity education that goes beyond theoretical knowledge. It is evident that while students may have a basic understanding of what phishing is, this knowledge remains superficial without practical application. Therefore, there is a pressing need to design and implement an educational program that not only covers the theoretical aspects of phishing and broader cyber threats but also immerses students in real-life scenarios. Such an approach would involve interactive workshops, hands-on training sessions, and simulated phishing exercises that allow students to experience and practice identifying phishing attempts in a controlled environment. By engaging in these practical activities, students can develop the necessary skills to critically evaluate email communications, recognize subtle cues of deception, and adopt safer digital habits. Moreover, this educational strategy should aim to bring about a significant behavioral change, fostering a proactive cybersecurity culture where students are consistently vigilant and prepared to mitigate potential phishing threats. This comprehensive, practice-oriented training is essential for reducing phishing susceptibility and strengthening the overall cybersecurity posture of the academic community.

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Summary

This study set out to investigate the susceptibility of students at the University of Benin (UNIBEN) to phishing attacks, with a view toward promoting sustainable and safe email usage within the academic environment. The research was guided by several key objectives: assessing students' awareness of phishing, identifying common phishing tactics, evaluating the effectiveness of existing cybersecurity measures, determining the factors that contribute to vulnerability, and analyzing the impact of demographic variables on susceptibility.

A mixed-methods research design was employed to capture a comprehensive picture of the issue. Quantitative data were gathered through surveys that measured students' cybersecurity awareness and recorded their experiences with phishing incidents. Basic statistical analyses, including descriptive statistics and correlation analysis, revealed that while the average awareness score was moderate, a significant proportion of students had fallen victim to phishing attacks, and there was a weak negative relationship between awareness and susceptibility.

Qualitative data were collected via interviews, focus groups, and document analysis. These findings highlighted that many students have only a superficial understanding of phishing attacks, relying heavily on visual cues such as familiar logos and institutional branding, which often leads to over-trust. Moreover, there is a pronounced deficiency in practical cybersecurity training, with students expressing a strong desire for hands-on, real-life applications that could better prepare them for actual phishing threats. The current email system at UNIBEN was also found to have several limitations, such as basic spam filtering,

weak authentication mechanisms, and reactive security policies that fail to proactively prevent attacks.

5.2 Conclusion

Based on the findings, it is evident that the cybersecurity posture at UNIBEN, particularly concerning email usage, requires significant improvement. While there is a moderate level of basic awareness among students, this awareness does not translate into effective protection against sophisticated phishing attacks. The research indicates that the reliance on superficial cues and the absence of practical, experiential learning contribute to a higher vulnerability among students.

Furthermore, the current security measures in place, including basic spam filters and password-based authentication, are not sufficient to counteract the evolving tactics used by cybercriminals. The qualitative insights reveal that a reactive approach to cybersecurity, combined with an institutional culture that does not prioritize continuous learning and proactive prevention, exacerbates the risks. Additionally, demographic factors such as year of study and email usage frequency play a role in influencing susceptibility, suggesting that a one-size-fits-all approach to cybersecurity training may not be effective.

The limitations of this study include a reliance on self-reported data, which may be subject to bias, and constraints in generalizing the findings beyond UNIBEN due to the specific institutional context. Nevertheless, the insights gained provide a strong foundation for developing targeted interventions aimed at reducing phishing susceptibility and enhancing overall cybersecurity awareness.

5.3 Recommendations

Based on the study's findings and implications, the following recommendations are proposed to improve the safety of email usage at UNIBEN:

1. **Implement Comprehensive Cybersecurity Training Programs:**
    - Develop and integrate practical cybersecurity education into the curriculum, focusing on real-life phishing scenarios and hands-on exercises.
    - Organize regular workshops, simulated phishing exercises, and interactive seminars to keep students updated on the latest phishing tactics and prevention strategies.
    - Ensure training is tailored to different student groups, addressing the specific needs of vulnerable demographics (e.g., first-year students and heavy email users).
2. **Upgrade Technical Security Measures:**
    - Enhance email filtering mechanisms by adopting advanced, AI-powered spam filters capable of detecting sophisticated phishing emails.
    - Implement multi-factor authentication (MFA) across the university's email system to add an extra layer of security and reduce the risk of unauthorized access.
    - Regularly update security protocols and ensure that the system is protected against emerging threats through continuous patch management.
3. **Establish a Formal Incident Reporting System:**
    - Create a structured, easily accessible platform for students and staff to report suspicious emails and phishing attempts.

- Develop clear guidelines and protocols for responding to reported incidents, ensuring prompt investigation and resolution.
- Use incident reports to inform continuous improvements in cybersecurity measures and training programs.

4. **Revise and Strengthen Institutional Cybersecurity Policies:**
   - Review current email security policies to identify gaps and align them with best practices in cybersecurity.
   - Formulate proactive policies that emphasize prevention rather than just reactive measures.
   - Incorporate mandatory cybersecurity awareness and training sessions as part of the university's policy for both new and returning students.
5. **Promote a Culture of Cybersecurity Awareness:**
   - Foster a campus-wide culture where cybersecurity is a shared responsibility through ongoing awareness campaigns, posters, digital newsletters, and social media engagement.
   - Encourage the formation of student-led cybersecurity clubs or committees that can provide peer-to-peer education and support.
   - Engage faculty and administration in promoting cybersecurity best practices and integrating these values into everyday academic and administrative activities.
6. **Monitor and Evaluate Effectiveness:**
   - Conduct regular assessments and surveys to monitor changes in cybersecurity awareness and phishing susceptibility over time.

- Use the data gathered from these evaluations to refine training programs and technical measures, ensuring they remain effective against evolving phishing tactics.
- Establish key performance indicators (KPIs) to measure the success of implemented interventions and adjust strategies accordingly.

REFERENCES

Fichtner, A., Spreitzenbarth, M., and Echtler, F. (2017). Clone phishing attacks: A comprehensive survey. *Journal of Computer Security*, 25(1), 31-68.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., and Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *In Proceedings of the SIGCHI conference on human factors in computing systems*: 26(8),373-382.

Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd.

Qbeitah, M. A., & Aldwairi, M. (2018, April). Dynamic malware analysis of phishing emails. In *2018 9th International Conference on Information and Communication Systems (ICICS)* (pp. 18-24). IEEE.

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications*, *182*(33), 27-29.

Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527-565.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*, 1-10.

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, *15*(4), 2070-2090.

Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*, *25*(5), 593-613.

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in psychology*, *11*, 1755.

Banu, M. N., & Banu, S. M. (2013). A comprehensive study of phishing attacks. *International Journal of Computer Science and Information Technologies*, *4*(6), 783-786.

Tsow, A., & Jakobsson, M. (2007). Deceit and deception: A large user study of phishing. *Indiana University. Retrieved September*, *9*, 2007.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. *Group Decision and Negotiation*, *19*, 391-416.

Karamagi, R. (2022). A Review of Factors Affecting the Effectiveness of Phishing. *Computer and Information Science*, *15*(1).

Tian, C., Jensen, M. L., Bott, G., & Luo, X. (2024). The influence of affective processing on phishing susceptibility. *European Journal of Information Systems*, 1-15.

Abbas, A. (2024). Evolving Phishing Defense: Innovative Defense Mechanisms and Effective Measurement Strategies.

Kheruddin, M. S., Zuber, M. A. E. M., & Radzai, M. M. M. (2024). Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. *Authorea Preprints*.

Afridi, S. (2024). Revolutionizing Phishing Defense: A Comprehensive Overview of Defense Mechanisms and Measurement Strategies.

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

Albalawi, T. F. (2018). *Quantifying the Effect of Cognitive Biases on Security Decision-Making* (Doctoral dissertation, Kent State University).

Katuk, N., Ruhani, A. B., Malik, M., Mahamood, A. K., & Omar, M. S. A. (2024). Protecting Higher Learning Institutions from Phishing Attacks: A Staff Awareness Program. In *Intelligent Systems of Computing and Informatics* (pp. 114-132). CRC Press.

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564-584.

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). *International Journal of Sustainable Development & Planning*, *18*(1)

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373-382).

Aliyu, M., Bagarawa, M. U., Mu'azu, A. N., & Umar, M. T. (2023). Understanding phishing awareness among students in tertiary institutions and setting-up defensive mechanisms against the attackers. *CaJoST*, *5*(1), 22-31.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & information technology*, *33*(3), 237-248.

Azad, R. U., Tasmim, S., & Atikuzzaman, M. (2025). Investigating students' awareness of online privacy and cybersecurity: an empirical study with effective cybersecurity training framework. *Global Knowledge, Memory and Communication*.

Tchakounté, F., Wabo, L. K., & Atemkeng, M. (2020). A review of gamification applied to phishing.

Khairallah, O., & Abu-Naseer, M. M. (2024). The effectiveness of gamification teaching method in raising awareness on Email Phishing: Controlled Experiment.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009, July). School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 1-12).

Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PloS one*, *14*(12), e0224216.

Gangavarapu, T., Jaidhar, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review*, *53*(7), 5019-5081.

Navaneeth, J., Rahaman, M., & Gupta, B. B. (2025). Anti-Phishing Technologies and Tools. In *Critical Phishing Defense Strategies and Digital Asset Protection* (pp. 121-148). IGI Global Scientific Publishing.

Chaudhary, S. (2016). The use of usable security and security education to fight phishing attacks.

Henriksson, A. (2022). What are the motivations and barriers for incorporating multi-factor authentication among IT students?.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International journal of information management*, *29*(6), 449-457.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*, 3629-3654.

Folorunso, A. (2024). Cybersecurity and its global applicability to decision making: a comprehensive approach in the university system. *Available at SSRN 4955601*.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Ellis, B. J., Del Giudice, M., Dishion, T. J., Figueredo, A. J., Gray, P., Griskevicius, V., ... & Wilson, D. S. (2012). The evolutionary basis of risky adolescent behavior: implications for science, policy, and practice. *Developmental psychology*, *48*(3), 598.

Juma, C., & Clark, N. (2002). Technological catch-up: Opportunities and challenges for developing countries. *SUPRA Occasional Paper, Research Centre for the Social Sciences, University of Edinburgh*, 1-24.

Alseadoon, I. M., Ramadan, R. A., & Khedr, A. Y. (2017). Cultural impact on users' ability to protect themselves against phishing websites. *International Journal of Computer Science and Network Security*, *17*(11), 1-5.

Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., ... & Ahn, G. J. (2020). Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*.

APPENDIX

SPECIMEN OF QUESTIONNAIRE

Objective 1: Assess the level of awareness among UNIBEN students regarding phishing attacks

1. Have you heard of the term "phishing" before?
   - Yes
   - No
2. How would you define phishing? (Open-ended question)
3. Have you ever received a phishing email or message?
   - Yes
   - No
   - I don't know
4. How confident are you in identifying a phishing email?
   - Very confident
   - Somewhat confident
   - Not very confident
   - Not at all confident

Objective 2: Identify common tactics used by cybercriminals to target students through email

1. Have you ever received an email that asked you to:

- Verify your account information?

- Click on a suspicious link?

- Download an attachment?

- Provide sensitive information?

- I don't know

2. How often do you receive emails that you consider spam or phishing attempts?

- Daily

- Weekly

- Monthly

- Rarely

- I don't know

3. What types of emails do you think are most likely to be phishing attempts? (Select all that apply)

- Emails asking for personal information

- Emails with urgent or threatening messages

- Emails with suspicious links or attachments

- Emails with spelling or grammar mistakes

- I don't know

Objective 3: Evaluate the effectiveness of existing cybersecurity measures in UNIBEN

1. Are you aware of any cybersecurity measures implemented by UNIBEN to protect students from phishing attacks?

- Yes
- No

2. How effective do you think these measures are in preventing phishing attacks?

- Very effective
- Somewhat effective
- Not very effective
- Not at all effective
- I don't know

3. Have you ever reported a phishing email or incident to UNIBEN's IT department?

- Yes
- No

Objective 4: Determine the factors contributing to students' susceptibility to phishing attacks

1. How often do you use public computers or public Wi-Fi networks to access your email or online accounts?

- Daily
- Weekly

- Monthly

- Rarely

2. Do you use the same password for multiple online accounts?

- Yes

- No

3. How confident are you in your ability to identify and avoid phishing attacks?

- Very confident

- Somewhat confident

- Not very confident

- Not at all confident

- I don't know

Objective 5: Propose strategies for enhancing cybersecurity awareness and safe email practices among students

1. What do you think would be the most effective way to educate students about phishing attacks and cybersecurity best practices? (Select all that apply)

- Workshops or training sessions

- Online resources or tutorials

- Email campaigns or newsletters

- Social media awareness campaigns

2. Would you be interested in participating in a cybersecurity awareness program or workshop?

- Yes

- No

3. Do you think UNIBEN should implement any of the following measures to enhance cybersecurity awareness? (Select all that apply)

- Mandatory cybersecurity training for students

- Regular phishing simulation exercises

- Cybersecurity awareness campaigns on social media

- Rewards or incentives for reporting phishing incidents

- I don't know

Objective 6: Analyze demographic factors that influence phishing susceptibility among students

1. What is your age?

- 18-20

- 21-23

- 24-26

- 27 or older

2. What is your faculty or department?

(Open end)

3. What is your level of study?

- Undergraduate

- Graduate

- Postgraduate

4. How often do you use email or online services for academic purposes?

- Daily

- Weekly

- Monthly

- Rarely