ENHANCING PHISHING AWARENESS AND PREVENTION THROUGH USER EDUCATION AMONG NIGERIAN STUDENTS

BY

NWACHUKWU CALEB PRECIOUS

20191156722

SUBMITTED TO

DEPARTMENT OF CYBER SECURITY, SCHOOL OF INFORMATION COMMUNICATION TECHNOLOGY

FEDERAL UNIVERSITY OF TECHNOLOGY, OWERRI, P.M.B 1526,

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF TECHNOLOGY IN CYBER SECURITY

SEPTEMBER, 2024

CERTIFICATION

This to certify that this project titled: **ENHANCING PHISHING AWARENESS AND PREVENTION THROUGH USER EDUCATION AMONG NIGERIAN STUDENTS** was carried out by **NWACHUKWU CALEB PRECIOUS (20191156722)** under the supervision of **DR. MRS. OKOLOEGBO CHRISTIANA** of the Department of Cyber Security, Federal University of Technology, Owerri.

....

Dr. Mrs. Okoloegbo Christiana **Date**

(Project Supervisor)

....

Date

(HOD, Department of Cyber Security)

....

Date

(DEAN OF SCIT)

....

EXTERNAL EXAMINER **Date**

TABLE OF CONTENT

ABSTRACT

Phishing attacks pose a significant threat to cybersecurity, exploiting users' lack of awareness to steal sensitive information. This study investigates the development and implementation of a Phishing Awareness System aimed at educating Nigerian students about phishing attacks and enhancing their ability to recognize and respond to such threats. The system consists of three key components: an Admin Login Page, an Awareness Page, and a Mock Phishing Form, each designed to simulate phishing scenarios and provide educational content. The study begins by evaluating the baseline knowledge of 120 student participants, revealing that 78 students (65%) were initially susceptible to phishing attacks. Following exposure to the awareness program, participants were assessed through a quiz, with 45 students (37.5%) scoring above 90%, and the remaining participants achieving scores between 65-80%. This improvement demonstrates the effectiveness of the system in raising awareness and equipping users with the skills necessary to detect phishing attempts. The development process involved creating an interactive platform, which simulates phishing attacks and educates users through quizzes and informative content. The system's architecture, entity relationship diagram, and flowchart were meticulously designed to ensure a seamless user experience and efficient data handling. Comprehensive testing and validation of the system confirmed its reliability and educational impact. Feedback from users highlighted increased confidence in identifying phishing attacks and a greater understanding of preventive measures. The study concludes by recommending the integration of phishing awareness programs into educational curricula, regular updates to the system, and the expansion of the user base to include diverse demographics.

Keywords: Phishing Awareness, Cybersecurity Education, Phishing Simulation, User Education, Nigerian Students, Cybersecurity Threats, User Engagement, Phishing Prevention, Cybersecurity Awareness Program.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Phishing is one of the most significant cybersecurity threats facing internet users today. It is a form of social engineering that uses manipulation and trickery to deceive individuals into revealing sensitive information or providing unauthorized access to systems (Hadnagy, 2021). Cybercriminals create phishing emails, often disguised as legitimate communication from trusted organizations, to exploit user vulnerabilities. These attacks are particularly dangerous because they do not necessarily require technical expertise—phishing software packages are easily available online (Bhardwaj & Sharma, 2020).

The success of phishing attacks is often influenced by the extent to which users can detect and respond to potential threats. Despite the design of socio-technical systems—such as internet browsers and email systems—that aim to protect users from external attackers, the effectiveness of these systems relies heavily on user engagement and decision-making (Pfeffel *et al.*, 2019). Users may fail to recognize cues provided by these systems or may not fully process the warning signs of a phishing attempt (Jansen & Van Schaik, 2019).

Research shows that people often rely on cognitive shortcuts, or decision-making heuristics, when interacting with digital platforms. Instead of thoroughly evaluating all the information available, individuals may make quick decisions based on a limited set of factors. This cognitive miser approach, although efficient, increases the risk of falling victim to phishing attacks, which often exploit urgency, fear, or financial concerns to trigger rapid, less analytical decision-making

(Gigerenzer & Brighton, 2019; Hadnagy, 2021). The language used in phishing emails frequently includes emotional triggers that encourage targets to act without fully processing the situation, leading to mistakes and security breaches (Goel & Jain, 2021).

In Nigeria, the increasing reliance on digital platforms, particularly among students in tertiary institutions who use these platforms for education, communication, and financial transactions, makes the need for effective phishing prevention education even more pressing. Despite the rapid growth of digital technology in the country, cybersecurity education remains underdeveloped, leaving students particularly vulnerable to these types of attacks. Additionally, phishing attacks are becoming more sophisticated, and there are no practical, user-focused cybersecurity training programs to address this gap (Olufowobi *et al.*, 2020).

This study seeks to address this gap by developing an innovative phishing simulation tool, specifically designed to educate Nigerian students on phishing awareness and prevention. By simulating real-life phishing scenarios, the tool will equip students with the knowledge and skills needed to recognize and respond to phishing threats.

1.2 Statement of Problem

Phishing, a widespread form of social engineering, is one of the most dangerous cybersecurity threats today. As Nigerian students increasingly rely on digital platforms for academic, social, and financial activities, they are becoming more vulnerable to these attacks. However, there is a significant lack of formal cybersecurity education and awareness programs in Nigeria, leaving students exposed to phishing and other cyber threats (Olufowobi *et al.*, 2020; Ogunleye, 2020). Phishing attacks exploit psychological tendencies, causing students to respond hastily to fraudulent emails, often without fully evaluating the potential risks (Olatunji, 2021). The

problem is compounded by students' limited technical knowledge and lack of awareness, making it difficult for them to recognize phishing attempts (Oshio & Aranu, 2021).

Despite the growing threat, there are few educational resources in Nigeria that focus on teaching students how to avoid phishing attacks. Most cybersecurity education lacks practical training that reflects real-world scenarios, leaving students unprepared (Adekoya *et al.*, 2020). This study aims to fill this gap by developing a phishing simulation tool to provide Nigerian students with hands-on experience in identifying phishing attempts, thereby improving their awareness and reducing their vulnerability to such threats.

1.3 Aim and Objectives of the study

The primary aim of this study is to enhance phishing awareness and improve phishing prevention among Nigerian students through the development and implementation of a phishing simulation. In doing so, the study will also review and build on existing literature to address current knowledge gaps in phishing awareness and prevention strategies, particularly within the Nigerian context.

The specific objectives are:

1. To evaluate the current level of awareness and knowledge of Nigerian students regarding phishing attacks and the associated risks.

2. To develop a phishing simulation tool.

3. To assess the effectiveness of the phishing simulation tool in improving students' ability to detect phishing attacks and respond appropriately.

1.4 Research questions

1. How knowledgeable are Nigerian students about phishing attacks?

2. How effective is the phishing simulation tool in improving students' ability to recognize phishing attempts?

3. What online behaviour changes are observed after students use the phishing simulation tool?

1.5 Scope of Study

This study focuses on Nigerian students in tertiary institutions, specifically those who use digital platforms regularly for educational, social, and financial activities. The research will involve the design, development, and implementation of a phishing simulation tool, to assess the effectiveness of phishing awareness and prevention education. The study will also evaluate the knowledge, behavior, and attitudes of students toward phishing attacks before and after participating in the simulation program. While the study will focus on Nigerian students, its findings may be applicable to other regions with similar educational and digital environments.

1.6 Limitation of Study

This study focuses on a specific group of Nigerian students in a tertiary institution, which may not fully represent the broader student population across Nigeria. Consequently, the results may have limited applicability to students in other regions or those not engaged in higher education. Additionally, some students may face technological barriers, such as limited access to computers or stable internet connections, which could restrict their participation in the phishing simulation and impact the study's reach, especially in areas with limited technological infrastructure.

Another limitation lies in the reliance on international literature to establish the study's theoretical foundation and methodology, as there is a lack of Nigeria-specific research on phishing. While phishing is a global issue, the absence of locally relevant studies may limit the cultural specificity of the findings. Furthermore, time constraints prevent long-term follow-up, which would have assessed the lasting impact of the phishing simulation. Finally, data privacy concerns restrict the types of phishing scenarios used, which may limit the depth of phishing attack simulations to protect participants' personal data.

1.7 Significance of the Study

This study is significant because it addresses a critical gap in cybersecurity education among Nigerian students, a group that is increasingly reliant on digital platforms for academic, social, and financial activities. Despite the growing use of technology in education, there is a lack of targeted, practical cybersecurity training that equips students with the necessary skills to identify and prevent cyber threats, particularly phishing attacks. Phishing remains one of the most prevalent forms of cybercrime globally, and Nigerian students are particularly vulnerable due to the absence of formal cybersecurity awareness programs.

By developing an interactive phishing simulation tool, this study will provide students with hands-on experience in recognizing phishing attempts and responding appropriately. Unlike theoretical learning, the simulation will mimic real-world scenarios, offering a more immersive learning experience. This practical approach will help students to internalize key concepts of phishing prevention, improving their ability to detect fraudulent emails, websites, and other online threats. In turn, this will reduce their risk of falling victim to cybercrime, protecting their personal, academic, and financial information.

The significance of this study extends beyond its immediate impact on students. The research will contribute to the growing body of knowledge on effective phishing prevention methods, offering insights into the effectiveness of simulation-based training in improving cybersecurity awareness. The findings could serve as a model for integrating phishing awareness into the educational curricula of Nigerian institutions, providing a framework for other universities and schools to adopt. This study's focus on experiential learning could inspire broader educational reform by incorporating user-focused cybersecurity education into general curricula.

Moreover, the results of this study could have broader implications for policymakers, educators, and technology developers. The insights gained from this research can help inform the development of national cybersecurity policies, highlighting the importance of proactive education in combating cyber threats. Educational institutions may be encouraged to adopt more interactive and practical approaches to teaching cybersecurity, while technology developers could use these findings to create more intuitive tools and platforms that protect users from phishing and other threats.

In summary, this study will not only provide Nigerian students with vital cybersecurity skills but will also contribute to the global fight against cyber threats by offering a scalable model for cybersecurity education.

CHAPTER TWO

LITERATURE REVIEW

2.1 Conceptual Framework

This section examines the major concept of phishing, as well as the study's historical and developmental trends.

2.1.1 Definition of Phishing

Phishing involves sending fraudulent messages that appear to come from trusted sources, such as large brands, banks, payment services, or postal services. These messages often mimic legitimate notifications and are nearly indistinguishable from real ones. They typically contain a message with a link to a fake resource, prompting the victim to follow the link and provide confidential information by filling out a form (Evglevsky *et al.*, 2021).

For example, scammers may impersonate a bank, sending fake messages to customers that resemble official communication. These messages inform the recipient that their account has been disabled and instruct them to click a link to restore access. The victim, driven by fear, may enter their banking details, allowing the scammer to steal their financial information (Olatunji, 2021).

Phishing is a type of cyberattack where malicious actors impersonate legitimate entities to deceive users into divulging sensitive information such as usernames, passwords, and financial details (Jagatic *et al.*, 2020). The term originates from the analogy of "fishing," where cybercriminals cast out fake bait to lure unsuspecting victims. Phishing attacks are primarily

carried out via emails, social media platforms, fake websites, and instant messaging services (Gupta *et al.*, 2021).

Modern definitions of phishing highlight its evolution into sophisticated forms, combining social engineering and technical tactics to exploit both psychological and technical vulnerabilities (Jansen & Van Schaik, 2019).

As cybercriminals become more advanced in their techniques, phishing remains one of the most prevalent and effective forms of cyber fraud globally.

2.1.2 Evolution and Techniques of Phishing

Phishing techniques have evolved considerably since the early 2000s, moving beyond basic email schemes to more sophisticated forms such as spear phishing, whaling, and smishing (SMS phishing).

1. **Spear Phishing**: This form of phishing targets specific individuals or organizations, often using personalized information to increase credibility (Jansson & Solms, 2020). Spear phishing attacks are particularly dangerous because they often go undetected and are tailored to exploit the target's specific weaknesses.
2. **Whaling**: A more focused type of phishing aimed at senior executives or high-profile targets within organizations. Whaling emails tend to be more sophisticated and often mimic official communications (Gupta *et al.*, 2021).
3. **Smishing and Vishing**: Smishing (SMS phishing) and vishing (voice phishing) are relatively recent developments where attackers use text messages or voice calls to deceive victims into sharing sensitive data (Harrison & Vishwanath, 2021).

2.1.3 Factors Contributing to Phishing Vulnerability

Several factors contribute to individuals' susceptibility to phishing attacks, including:

1. **Lack of Awareness**: Many individuals, particularly students, lack awareness of phishing techniques, leaving them vulnerable to these forms of cyberattacks (Oshio & Aranu, 2021).
2. **Technological Gaps**: The rapid adoption of digital platforms without adequate user training on cybersecurity creates opportunities for cybercriminals to exploit weak points (Harrison & Vishwanath, 2021).
3. **Psychological Manipulation**: Phishing schemes rely heavily on manipulating human psychology, such as inducing fear, urgency, or excitement to provoke immediate responses (Jansson & Solms, 2020).

2.1.4 The Importance of User Education

User education has become an essential component of cybersecurity strategies aimed at mitigating the risks associated with phishing (Jansen & Van Schaik, 2019). Phishing awareness programs aim to ensure that users, especially students who are often the target of cyberattacks, can act as the first line of defense. By equipping users with the knowledge to recognize phishing attempts and training them on how to respond appropriately, the susceptibility to these attacks can be significantly reduced (Alotaibi *et al.*, 2021).

In Nigeria, the proliferation of digital services and mobile technologies makes students particularly vulnerable to phishing scams. Many students lack the cybersecurity awareness necessary to protect themselves from fraudulent schemes, thus creating a critical need for

targeted educational interventions (Oshio & Aranu, 2021). As Nigerian universities embrace e-learning platforms, online banking, and social media, the need for cybersecurity education, particularly on phishing prevention, becomes increasingly urgent.

2.1.5 Studies on Phishing Awareness

Empirical research has demonstrated that phishing awareness programs are highly effective in reducing users' vulnerability to phishing attacks. For example, a study by Jansen and Van Schaik (2019) found that participants who received phishing awareness training were significantly less likely to fall for phishing scams than those who had not received such training. The study highlighted that practical, hands-on training with real-life examples of phishing emails enhanced participants' ability to detect phishing attempts.

A similar study by Alotaibi *et al.* (2021) examined the impact of phishing awareness programs on university students and found that interactive modules and phishing simulations were the most effective educational methods. Students who participated in simulated phishing scenarios were better equipped to recognize suspicious behavior and were more confident in their ability to avoid phishing attacks. The findings suggested that immersive educational experiences should be central to phishing awareness programs in higher education.

2.1.6 Nigerian Context of Phishing Education

In Nigeria, the rise in internet access and mobile device usage has made students prime targets for phishing attacks. Oshio and Aranu (2021) found that phishing awareness among Nigerian tertiary institution students was relatively low, and many were unaware of the latest phishing techniques. However, after introducing a structured phishing awareness campaign, students'

ability to identify phishing attempts increased by over 40%, demonstrating the effectiveness of tailored educational interventions.

Moreover, Gupta *et al.* (2021) conducted a meta-analysis of global phishing awareness programs and found that continuous education is necessary for long-term protection, as phishing tactics continuously evolve. The study indicated that one-time training sessions are insufficient, stressing the importance of regular updates and practical reinforcement for maintaining phishing awareness among students.

2.1.7 Practical Implications for Phishing Prevention

The empirical evidence points to several practical implications for improving phishing awareness among Nigerian students. First, educational programs should incorporate interactive simulations mimicking real-world phishing attacks, as these have been shown to be the most effective method for enhancing phishing detection (Alotaibi *et al.*, 2021). Second, ongoing education is essential, as one-off training programs may not provide sufficient reinforcement for long-term retention of phishing prevention skills (Gupta *et al.*, 2021). Finally, phishing education should be integrated into broader digital literacy curricula in Nigerian universities to ensure all students receive consistent cybersecurity training (Oshio & Aranu, 2021).

2.1.8 The Impact of Phishing on Individuals and Institutions

Phishing can have severe consequences for both individuals and institutions. Students, in particular, are often targeted because they may be less familiar with cybersecurity measures. They may unknowingly reveal sensitive information, such as bank details or academic credentials, which can be used for identity theft or financial fraud (Bhardwaj & Sharma, 2020). For educational institutions, phishing attacks can lead to data breaches compromising student

records, research data, and financial information. These breaches can result in financial losses, legal liabilities, and reputational damage, as seen in recent attacks targeting universities globally (Jalali *et al.*, 2020).

In Nigeria, phishing attacks are increasingly prevalent, with both individuals and organizations falling victim to sophisticated schemes. A notable example is the 2021 case involving Nigerian universities where cybercriminals targeted students with fraudulent emails, claiming to offer scholarships and financial aid (Umeh, 2021). Many students, eager to secure financial assistance, fell prey to these scams, revealing their personal and financial details. These kinds of attacks exploit students' financial vulnerability and lack of awareness about phishing. Similarly, institutions in Nigeria, including banks and governmental organizations, have been targeted by large-scale phishing attacks that compromise financial systems and expose critical data. The 2020 phishing attack on a Nigerian financial institution led to the theft of millions of naira from customer accounts, illustrating the significant financial impact such incidents can have on national economies (Ogunleye, 2020).

Globally, phishing continues to be one of the most common and damaging types of cyberattacks. The infamous 2021 phishing attack on the Democratic National Committee (DNC) in the United States, which led to the leak of thousands of emails, demonstrated the potential for phishing to influence not just individuals or organizations, but entire political processes (Menn, 2021). This attack, believed to be orchestrated by foreign state actors, had far-reaching consequences for the U.S. election system and exposed the vulnerabilities in both institutional and individual cybersecurity practices.

2.1.9 Phishing Awareness among Students

Phishing awareness among students is crucial, as students are frequent targets of cybercriminals due to their often limited knowledge of cybersecurity practices and their heavy reliance on digital communication platforms. Several studies have been conducted to assess the level of phishing awareness among students, with varying results based on the region and demographic. In general, studies indicate that while many students are aware of the term "phishing," they often lack the deeper understanding needed to recognize phishing attempts or know how to respond to them appropriately (Harrison *et al.*, 2021).

A study conducted by Jansen and Van Schaik (2019) found that among college students in the United States, around 70% had encountered phishing emails, yet only 45% could correctly identify the hallmarks of a phishing attempt. The study revealed that although students were aware of the basic concept of phishing, they struggled to differentiate legitimate communications from fraudulent ones. Similarly, a European study by Goel and Jain (2021) demonstrated that even though 85% of university students reported being aware of phishing, over 60% admitted to having clicked on a phishing link at some point, underscoring a disconnect between awareness and behavioral response.

In the Nigerian context, phishing awareness among students is even lower, with a greater need for cybersecurity education and preventive measures. Studies in Nigeria reveal significant gaps in students' understanding of phishing and other cybersecurity threats. A survey by Olufowobi *et al.* (2020) on cybersecurity awareness among Nigerian university students showed that less than 40% of respondents could identify phishing emails, and even fewer understood the potential consequences of phishing attacks. Most students lacked formal education or training in

cybersecurity, relying instead on informal knowledge, which left them vulnerable to increasingly sophisticated phishing tactics.

Moreover, the reliance on mobile devices for internet access among Nigerian students introduces additional vulnerabilities. According to a report by Olatunji (2021), the high use of mobile devices, coupled with a lack of robust cybersecurity tools on those devices, increases the likelihood of students falling victim to phishing attacks. Many students do not have access to comprehensive antivirus software or are unaware of how to implement basic security measures, such as enabling multi-factor authentication or verifying suspicious links. This highlights a critical gap in phishing awareness, particularly as mobile phishing, which targets text messages and apps, becomes more prevalent.

Additionally, there is a gap in institutional support for phishing education in Nigerian universities. While some institutions offer general IT courses, cybersecurity training is rarely included as a mandatory part of the curriculum. As a result, students often lack the formal training needed to recognize phishing attempts, leaving them exposed to attacks that could compromise their personal data and financial security (Adeniran *et al.*, 2019). This gap in cybersecurity education underscores the need for more targeted initiatives that focus specifically on phishing and other forms of online fraud, especially as digital learning and online communication continue to grow in importance in academic settings.

2.1.10 Cybersecurity Awareness Programs in Nigeria

In response to the rising tide of cybercrime and phishing attacks, several government and institutional initiatives have been launched in Nigeria to improve cybersecurity awareness, particularly among students. These efforts are critical in a country where the digital economy is

expanding rapidly, and students, who make up a significant portion of the internet-using population, are increasingly at risk of cyberattacks. While these initiatives have made some progress, challenges remain in their effective implementation.

2.1.11 Government Initiatives

The Nigerian government has been proactive in creating a legal and regulatory framework to promote cybersecurity awareness. The *Cybercrime Act of 2021* was a significant step in defining cybercrime and prescribing penalties for cybercriminals. This legislation laid the groundwork for cybersecurity awareness by recognizing the importance of public education in preventing cyber threats. Additionally, the *National Information Technology Development Agency (NITDA)* has been at the forefront of promoting cybersecurity awareness. NITDA has organized workshops, seminars, and campaigns aimed at educating students and the general public about the risks of cyber threats, including phishing, and best practices for staying secure online (NITDA, 2019).

One of the most notable government-led initiatives is the *CyberSafeNG* project, launched in partnership with the Central Bank of Nigeria (CBN) and several private sector organizations. This program focuses on raising awareness about phishing and other forms of cybercrime by targeting students and youth through social media campaigns, school-based cybersecurity clubs, and educational webinars. CyberSafeNG has also developed e-learning resources to improve cybersecurity literacy among students, providing materials that teach basic concepts like identifying phishing emails and securing personal devices (CyberSafeNG, 2021).

2.1.12 Institutional Initiatives

Within the educational sector, several Nigerian universities and polytechnics have begun implementing cybersecurity awareness programs aimed at students. Many universities now offer

cybersecurity as part of their information technology (IT) curriculum, while others have set up student-led cybersecurity clubs. These clubs organize awareness campaigns and host training sessions to help students understand the growing threats of phishing and other cybercrimes (Adekoya *et al.*, 2020). Additionally, some institutions have introduced online platforms and portals where students can report phishing attempts or receive guidance on how to protect themselves from cyberattacks.

For example, the University of Lagos launched its *Cybersecurity Awareness Initiative* in collaboration with tech companies like Microsoft and Kaspersky Lab. This program offers periodic training sessions and seminars on topics like phishing, password management, and the importance of data encryption. The university also encourages students to participate in national cybersecurity competitions, which help to build their knowledge and skills in preventing phishing attacks and other cyber threats (UNILAG Cybersecurity Center, 2020).

2.1.13 Challenges in Implementing Cybersecurity Awareness Programs

Despite these efforts, several challenges hinder the effectiveness of cybersecurity awareness programs in Nigeria. One of the primary obstacles is the lack of adequate funding. Both government and institutional initiatives often struggle with financial constraints, limiting the reach and scope of cybersecurity education programs. Many universities, particularly those in rural areas, lack the resources to set up comprehensive cybersecurity awareness campaigns, leaving students in these regions more vulnerable to phishing attacks (Adeniran *et al.*, 2019).

Another challenge is the low level of digital literacy among students and educators. Many Nigerian students, especially those in non-urban areas, have limited access to computers and the internet, making it difficult for them to engage with cybersecurity content. Furthermore, many

educators are not trained in cybersecurity, which means they are unable to effectively teach students how to recognize phishing attempts or employ protective measures. This gap in digital literacy has slowed the progress of government and institutional programs aimed at boosting cybersecurity awareness (Olatunji, 2021).

Cultural attitudes toward cyber threats pose a barrier. In some communities, there is a general lack of urgency regarding cybersecurity, with many viewing cyberattacks as distant or irrelevant threats. This complacency makes it harder to engage students and convince them to take phishing and other cyber threats seriously. Without a shift in cultural attitudes, awareness campaigns face an uphill battle in fostering long-term behavioral changes among Nigerian students (Ogunleye, 2020).

The rapid evolution of cyber threats presents another challenge. Cybercriminals continually develop new phishing tactics and other malicious techniques, making it difficult for awareness programs to keep pace with the latest threats. Students who may have learned about older forms of phishing may not be equipped to recognize more sophisticated attacks, such as those that exploit social media platforms or use AI-generated content to deceive victims (Umeh, 2021).

2.2 Theoretical Framework

Relevant theories relating to phishing have been studied in this section to increase understanding and provide a foundation for the proposed prevention tool or method development.

2.2.1 Protection Motivation Theory (PMT)

The Protection Motivation Theory (PMT) offers a useful framework for understanding phishing awareness and prevention. PMT posits that individuals are motivated to protect themselves based

on their assessment of the threat's severity and vulnerability, their belief in the efficacy of protective behaviors, and their confidence in executing these behaviors (self-efficacy) (Rogers, 1983 as cited in Milne *et al.*, 2020). In the context of phishing prevention among students, PMT suggests that raising awareness of the dangers of phishing and providing practical skills to mitigate these threats can enhance users' motivation to adopt safe online practices. If students perceive phishing as a serious threat and believe they can effectively avoid it by applying learned skills, they are more likely to take preventive measures (Milne *et al.*, 2020).

2.2.2 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) emphasizes the importance of perceived ease of use and perceived usefulness in the adoption of new technologies (Davis, 1989; Gupta *et al.*, 2021). Applied to phishing awareness programs, TAM suggests that students are more likely to engage with and retain cybersecurity knowledge if they find educational tools easy to use and relevant to their daily online activities. Interactive simulations or gamified phishing training modules that are user-friendly encourage higher participation rates among students (Gupta *et al.*, 2021). TAM supports the design of intuitive and practical educational tools to foster positive attitudes toward phishing prevention.

2.2.3 Theory of Planned Behaviour (TPB)

The Theory of Planned Behaviour (TPB) explains human behavior as a function of attitudes, subjective norms, and perceived behavioral control (Ajzen, 1991 as cited in Sheeran *et al.*, 2021). In phishing prevention, TPB suggests that students' intentions to avoid phishing attacks are shaped by their attitudes toward online security, the influence of their peers, and their confidence in identifying phishing attempts. Phishing awareness programs that foster a positive

attitude toward cybersecurity, create a normative culture that values online safety, and enhance students' self-efficacy can increase the likelihood of preventive behaviors (Sheeran *et al.*, 2021).

2.3 Empirical Framework

Recent empirical studies have highlighted the pressing need for enhanced phishing awareness and prevention among Nigerian students. A 2023 study conducted at Sokoto State University assessed students' awareness of phishing tactics, revealing that while many students were cautious about sharing personal information via email or SMS, they remained susceptible to other phishing strategies. The researchers emphasized the importance of comprehensive educational initiatives to bolster students' defenses against phishing attacks (Aliyu *et al.*, 2023).

Similarly, a 2024 study at the University of Abuja evaluated social engineering awareness among students through a pragmatic approach. The findings indicated a concerning lack of awareness, with 63% of respondents having no prior knowledge of social engineering and its attack vectors. Phishing emerged as the most prevalent attack vector, affecting 50% of respondents. The study underscored the urgent need for enhanced social engineering awareness and cybersecurity measures within the university community (Gift *et al.*, 2024).

Further emphasizing this issue, a 2023 study at a leading Nigerian university investigated students' susceptibility to phishing attacks. The results showed that 70.6% of surveyed students were susceptible to phishing attacks due to a lack of awareness. The study concluded with recommendations to secure the academic community and ICT infrastructures to achieve a sustainable and safe email usage environment (Okokpujie *et al.*, 2023).

Aliyu *et al.* (2023) conducted a study at Sokoto State University to assess students' awareness of phishing tactics. The research revealed that although many students exhibited caution in sharing personal information via email and SMS, they were still vulnerable to more sophisticated phishing techniques, such as cloned websites and fake login portals. The study emphasized the need for tailored educational initiatives to address these gaps, suggesting that interactive learning approaches like role-playing and phishing simulations could be particularly effective.

Gift *et al.* (2024) undertook an empirical study at the University of Abuja to evaluate students' understanding of social engineering, with phishing as a key focus area. The findings showed that 63% of the respondents had no prior knowledge of social engineering, and nearly 50% admitted to having fallen victim to phishing at some point. The study highlighted the role of targeted training programs and workshops in empowering students with practical knowledge about identifying phishing attempts. Furthermore, the research stressed the importance of integrating cybersecurity education into the university curriculum to foster a culture of digital vigilance.

Okokpujie *et al.* (2023) conducted a study to examine the susceptibility of Nigerian university students to phishing attacks. They discovered that 70.6% of students surveyed lacked the necessary knowledge and skills to identify phishing attempts. The authors attributed this susceptibility to inadequate exposure to cybersecurity training and recommended implementing widespread educational campaigns within academic institutions. They also called for collaboration between universities and tech organizations to deploy phishing simulation tools and provide hands-on training.

Building on this foundation, Adewole *et al.* (2021) explored the efficacy of digital literacy programs in reducing phishing incidents among Nigerian students. Their study found that

students who participated in targeted cybersecurity workshops demonstrated a 45% improvement in their ability to recognize phishing emails compared to those who did not receive such training. The researchers concluded that integrating digital literacy initiatives into academic programs could significantly reduce phishing-related risks.

Another significant contribution came from Musa *et al.* (2022), who examined the role of peer learning in enhancing cybersecurity awareness. Their study at Lagos State University highlighted that peer-based education programs, such as group discussions and student-led workshops, were effective in demystifying complex cybersecurity concepts for students. Participants reported feeling more confident in their ability to identify phishing attempts after engaging in peer learning sessions.

These studies collectively underline the importance of educational interventions tailored to the unique needs of Nigerian students. They suggest that a multipronged approach combining formal education, peer learning, and interactive training programs can significantly enhance phishing awareness and prevention. Furthermore, the findings indicate the need for collaboration among stakeholders, including universities, government agencies, and technology companies, to create a robust framework for cybersecurity education.

2.4 Summary of Literature

Title	Author (Year)	Problem	Method/Solution	Results
Impact of phishing awareness programs on university students	Alotaibi *et al.* (2021)	Low phishing awareness among students.	Interactive modules and phishing simulations were used.	Students became better equipped to recognize phishing and were more confident in avoiding attacks.
Phishing attacks and its impact on cyber security	Bhardwaj & Sharma (2020)	Cyberattacks causing financial and identity losses.	Reviewed phishing attack methods and countermeasures.	Identified methods for individuals and institutions to mitigate phishing attacks.
Cybersecurity awareness among Nigerian students	Oshio & Aranu\ (2021)	Low cybersecurity awareness among Nigerian students, leading to vulnerability to phishing attacks.	Structured phishing awareness campaigns.	Increased phishing recognition by 40% among students.
Defending against phishing attacks: taxonomy of methods	Gupta *et al.* (2021)	Constantly evolving phishing tactics.	Meta-analysis of phishing awareness programs.	Found continuous education to be critical for long-term protection against phishing.

Phishing awareness among students	Jansen & Van Schaik (2019)	Students struggle to identify phishing attempts despite encountering them.	Phishing awareness training including real-life examples of phishing emails.	Improved ability to detect phishing attempts among students.
Mobile phishing in Nigeria: vulnerabilities and impact	Olatunji (2021)	Mobile device users, especially students, are vulnerable to phishing due to lack of robust security tools.	Examined mobile phishing trends among Nigerian students.	Identified gaps in mobile security awareness and recommended educational interventions.

The reviewed literature reveals a consensus on the effectiveness of phishing awareness programs in reducing the risk of cyberattacks, particularly among vulnerable populations such as students. Conceptually, phishing remains a pervasive threat in the digital age, with users being the primary targets due to their limited cybersecurity awareness. Theories such as the Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), and Theory of Planned Behavior (TPB) provide a strong foundation for designing educational programs that empower users to protect themselves from phishing attacks.

Empirical studies consistently demonstrate that phishing awareness programs, particularly those that include interactive and practical components, are effective in improving phishing detection and prevention skills. In the Nigerian context, the rapid growth of digital services underscores the urgency of implementing targeted phishing education campaigns for students. These campaigns should be ongoing, culturally relevant, and incorporated into the broader digital

literacy efforts of educational institutions. Such initiatives can significantly reduce students' vulnerability to phishing, thereby enhancing overall cybersecurity.

2.4.1 Research Gap

While there is extensive research on phishing awareness and prevention, significant gaps exist in the application of these studies within the context of Nigerian students. Most existing literature is centered around corporate environments or higher-income countries, where access to resources and cybersecurity infrastructure differs markedly from that of developing nations (Ahmed *et al.*, 2021). There is limited empirical research assessing the effectiveness of phishing awareness programs tailored specifically to the educational sector in Nigeria. This gap is critical as students form a substantial portion of the online population and are increasingly targeted by cybercriminals due to their frequent internet usage and often limited cybersecurity knowledge (Eze *et al.*, 2022).

Furthermore, the lack of research on the long-term impact of educational interventions on students' cybersecurity behavior presents another significant gap. While short-term improvements in phishing detection capabilities are well-documented, there is insufficient evidence on the sustainability of these improvements over time and how they influence students' overall cybersecurity posture (Adebayo & Adekunle, 2023). This study aims to address these gaps by evaluating the current level of phishing awareness among Nigerian students and assessing the effectiveness of a simulation-based educational intervention designed to improve their ability to recognize and respond to phishing attacks.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Research Methodology Overview

This research focused on enhancing phishing awareness and prevention among Nigerian students through a systematic approach that included evaluating existing awareness levels, developing a simulation tool, and assessing its effectiveness. The study utilized a mixed-methods approach, combining both qualitative and quantitative techniques to comprehensively understand the issue of phishing among the target demographic. The methodology was designed to ensure the accurate collection, analysis, and interpretation of data to achieve the research objectives effectively. By integrating surveys, simulations, and evaluations, the study provided a robust framework for understanding and improving phishing awareness.

The initial phase involved a thorough review of existing literature on phishing and its impact on students. This review provided a foundational understanding of the common phishing tactics, student vulnerabilities, and existing educational interventions. The insights from this review informed the design of the study and the development of the simulation tool. The methodology was structured to first gauge the baseline awareness levels among students, followed by an intervention using a developed tool, and finally, an assessment to determine the tool's impact on the students' phishing detection capabilities.

3.2 Methodology Adopted

The research methodology was executed in several distinct stages, each contributing to the overall goal of improving phishing awareness and prevention among Nigerian students. The first

stage involved evaluating the current level of awareness and knowledge regarding phishing attacks and associated risks. A survey was administered to a representative sample of students in from the Federal University of Technology Owerri, Nigeria. The survey included questions designed to assess their understanding of phishing, their experiences with phishing attempts, and their ability to identify phishing threats. The data collected from these surveys provided a clear picture of the current state of phishing awareness among the student population.

In the second stage, the development of a phishing simulation tool was undertaken using an interactive platform that allows for the creation of realistic phishing scenarios aimed at educating users about phishing tactics. The tool was customized to reflect common phishing strategies that students might encounter, such as fake login pages and fraudulent emails. The development process involved scripting various phishing scenarios, creating mock interfaces, and embedding educational content that provides immediate feedback to users. This tool was designed to simulate a real-world phishing experience, thereby enhancing the practical learning aspect of the students' education.

The final stage involved assessing the effectiveness of the phishing simulation tool. This was done by deploying the tool among the same group of students who participated in the initial survey. After engaging with the simulation tool, students were re-evaluated through follow-up surveys and quizzes that measured their ability to detect phishing attacks and respond appropriately. The data from these evaluations were analyzed to determine the improvement in phishing awareness and detection skills among the students. Comparative analysis between pre- and post-intervention results provided insights into the effectiveness of the tool, highlighting areas of improvement and success in enhancing the students' cybersecurity awareness.

Throughout the study, data were collected and analyzed using statistical methods to ensure the reliability and validity of the findings. The results of this comprehensive methodological approach provided a clear indication of the current state of phishing awareness among Nigerian students and the potential of interactive educational tools like GeoPhish to significantly enhance their ability to recognize and respond to phishing threats.

3.3 Development Stages of the App

The development of the phishing awareness simulation app followed a structured and iterative approach to ensure its effectiveness in educating users and simulating real-world phishing scenarios. The development process was divided into several key stages, each focusing on specific aspects of the app's functionality and user experience.

Stage 1: Requirement Gathering and Analysis This initial stage involved collecting and analyzing the requirements for the app. The primary focus was on understanding the educational needs of Nigerian students regarding phishing awareness. Input was gathered from cybersecurity experts, educators, and potential users to define the core functionalities and desired outcomes of the app. The requirement analysis ensured that the app would meet the educational goals and provide a user-friendly experience.

Stage 2: Design and Prototyping Once the requirements were clearly defined, the design phase began. This stage involved creating wireframes and prototypes to visualize the app’s interface and user flow. The design emphasized simplicity and interactivity to engage users effectively. The prototypes were reviewed and refined based on feedback from stakeholders, ensuring that the final design would be intuitive and visually appealing.

Stage 3: Development The actual development of the app commenced after the design was finalized. The app was built using a combination of front-end and back-end technologies to support its interactive features. The development team implemented the core components, including the admin login page, the awareness page with educational content and quizzes, and the mock phishing form. Each component was developed incrementally, with continuous testing to ensure functionality and integration.

Stage 4: Testing and Quality Assurance Testing was a critical stage in the app development process. Various testing methods, including unit testing, integration testing, and user acceptance testing, were conducted to identify and resolve any bugs or issues. The focus was on ensuring the app was secure, reliable, and provided a seamless user experience. The feedback from test users was instrumental in making final adjustments and improvements to the app.

Stage 5: Deployment After thorough testing and validation, the app was deployed for use by the target audience. Deployment included setting up the necessary infrastructure to host the app and ensuring that it was accessible to users. Documentation and user guides were also prepared to assist users in navigating the app and making the most of its features.

Stage 6: Maintenance and Updates Post-deployment, the app entered the maintenance phase. This stage involves monitoring the app's performance, collecting user feedback, and making necessary updates and enhancements. Regular updates ensure that the app remains effective in addressing new phishing threats and continues to provide valuable educational content.

3.4 Implementation

The implementation of the phishing awareness system was a comprehensive process that involved various stages, from selecting the right development tools to building and integrating system components. Each component was designed to fulfill a specific role in achieving the overall goal of enhancing phishing awareness among students. The development environment and tools played a crucial role in ensuring that the system was robust, efficient, and user-friendly.

3.4.1 Development Tools and Environment

The development of the phishing awareness system was carried out in a versatile and well-structured environment to ensure smooth progress and high-quality output. The primary tools used included Visual Studio Code (VS Code) as the integrated development environment (IDE), which provided an efficient platform for coding, debugging, and testing. The system was built using standard web development technologies, including HTML, CSS, and JavaScript, which were chosen for their flexibility and widespread compatibility with web browsers. These technologies allowed for the creation of a dynamic and responsive user interface, crucial for engaging the target audience.

For version control, Git was employed, enabling the team to manage changes and collaborate effectively. This ensured that all updates were tracked, and any issues could be resolved efficiently. Additionally, localStorage was used for temporary data storage, facilitating quick data retrieval and session management during the development phase. The choice of localStorage was driven by the need for a lightweight solution that could handle the system's data requirements without the overhead of a full-fledged database.

3.4.2 System Components

The system was designed to have three main components: the Admin Login Page, the Awareness Page, and the Mock Phishing Form. Each component was developed to address specific aspects of phishing awareness, from administrative control to user education and simulation.

3.5 Functional Requirements

The functional requirements of the phishing awareness simulation app outline the essential features and capabilities that the app must possess to fulfill its purpose. These requirements ensure that the app provides a comprehensive and engaging learning experience for users, as well as administrative functionalities for managing and analyzing user interactions.

1. User Authentication

i. The app must provide a secure login mechanism for administrators.
ii. Only authenticated administrators should have access to the dashboard and user data.

2. Awareness Content Delivery

i. The app must include educational content on phishing, including definitions, types of attacks, and preventive measures.
ii. The content should be structured in a way that is easy to understand and engaging for students.

3. Interactive Quiz

i. The app must include a quiz with multiple-choice questions to assess users' understanding of phishing.
ii. The quiz should provide immediate feedback on answers, helping users learn from their mistakes.

4. Phishing Simulation

i. The app must simulate a phishing attack through a mock form that collects personal information.
ii. After form submission, users should be alerted that they have fallen victim to a phishing simulation, reinforcing the learning objective.

5. Data Storage and Retrieval

i. The app must store user data, such as quiz scores and submitted information from the mock form, securely.
ii. Administrators should be able to retrieve and review this data via the dashboard for analysis.

6. Admin Dashboard

i. The app must include an admin dashboard that displays user interactions, quiz results, and submitted data from the mock form.
ii. The dashboard should provide insights into user performance and the effectiveness of the educational content.

7. User-Friendly Interface

i. The app must have an intuitive and responsive user interface that is accessible on various devices.
ii. The design should facilitate easy navigation between the awareness page, quiz, and mock form.

8. Feedback and Support

i. The app must include mechanisms for users to provide feedback on their experience.
ii. It should also offer support features, such as FAQs or a help section, to assist users in case of difficulties.

3.6 Non-Functional Requirements

The non-functional requirements of the phishing awareness simulation app define the quality attributes and operational constraints that the system must adhere to. These requirements ensure that the app not only meets its functional objectives but also provides a reliable, secure, and user-friendly experience.

1. Performance

i. The app must respond to user actions within 2 seconds under normal usage conditions.
ii. It should be capable of handling up to 500 concurrent users without performance degradation.

2. Scalability

i. The app should be designed to accommodate growth in the number of users and data without requiring significant changes to the underlying architecture.
ii. It must support additional educational content and quiz modules as needed.

3. Security

i. The app must implement secure authentication mechanisms to protect administrator accounts.
ii. User data, including quiz results and mock form submissions, must be encrypted and stored securely to prevent unauthorized access.

4. Usability

i. The app must have a user-friendly interface that is intuitive for users with minimal technical knowledge.
ii. It should include clear instructions and feedback messages to guide users through the awareness content and quizzes.

5. Availability

i. The app must have an uptime of 99.9%, ensuring that it is accessible to users at all times.
ii. It should include redundancy mechanisms to recover quickly from any failures.

6. Maintainability

i. The app must be built with a modular architecture to facilitate easy updates and maintenance.
ii. Documentation should be provided for all components to assist in troubleshooting and future development.

7. Compatibility

i. The app must be compatible with major web browsers (e.g., Chrome, Firefox, Safari, Edge) and mobile devices.
ii. It should adhere to web standards to ensure cross-platform compatibility.

8. Accessibility

i. The app should be accessible to users with disabilities, following the Web Content Accessibility Guidelines (WCAG).
ii. Features such as keyboard navigation and screen reader support should be included.

9. Reliability

i. The app must provide consistent performance and reliability, even during peak usage periods.
ii. It should include error handling mechanisms to recover from unexpected issues gracefully.

10. Localization

i. The app should support multiple languages to cater to a diverse user base.
ii. It should allow for easy translation and adaptation of content as needed.

3.7 Use Case Diagram

This diagram shows the interactions between the user and the system, including login, accessing educational content, and participating in quizzes.

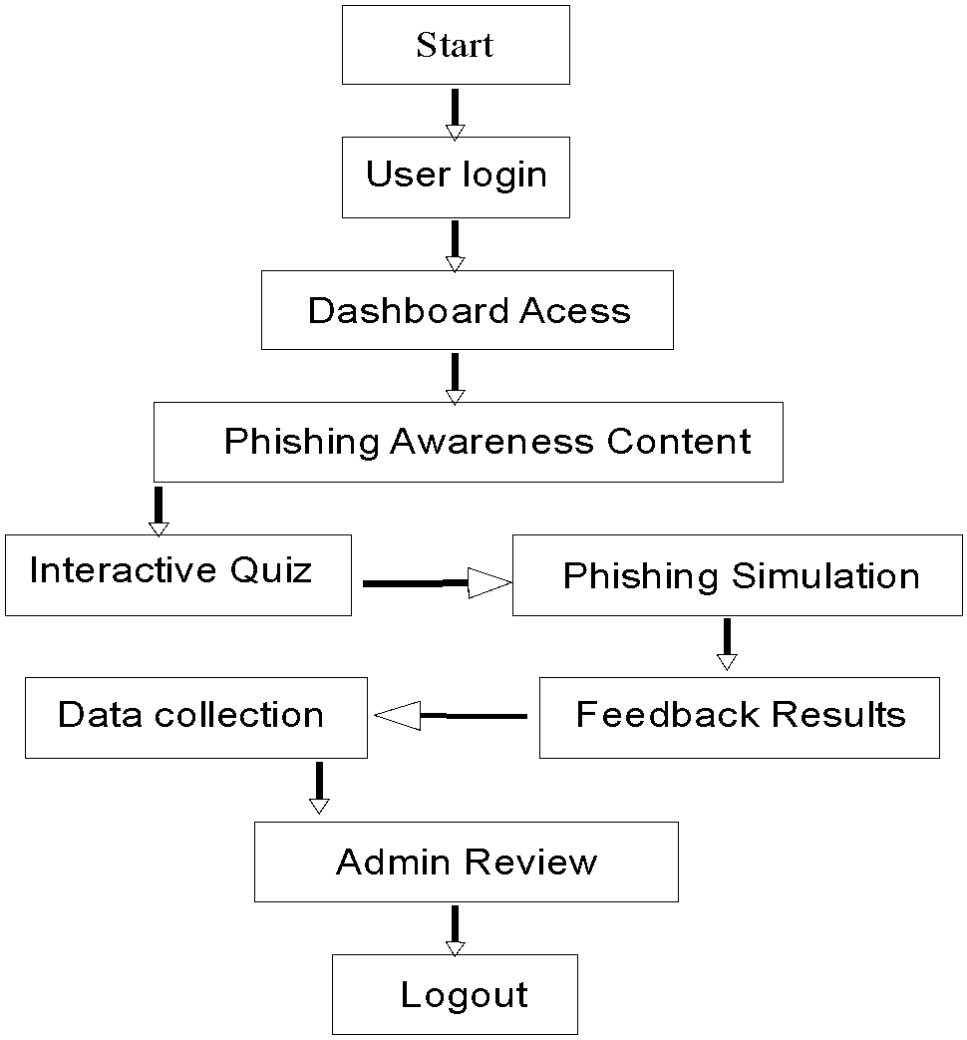

Figure 3.1: Use case diagram

3.8 Entity Relationship Diagram (ERD)

The Entity Relationship Diagram (ERD) for the phishing awareness simulation app visualizes the data entities, their attributes, and the relationships between them. This helps in understanding how data is structured and interconnected within the system. It illustrates the data structure and the relationships between different entities within the system. Key entities include Users, Admins, Quizzes, Questions, and Responses. The Users entity captures information about the individuals participating in the awareness program, such as their ID and interaction history. Admins are a separate entity, representing system administrators who manage content and oversee user engagement.

Entities:

i. **Administrator**
    a. Attributes: Admin_ID (Primary Key), Username, Password
ii. **Student**
    a. Attributes: Student_ID (Primary Key), Name, Email, Score
iii. **Quiz**
    a. Attributes: Quiz_ID (Primary Key), Question, Options, Correct_Answer
iv. **Response**
    a. Attributes: Response_ID (Primary Key), Student_ID (Foreign Key), Quiz_ID (Foreign Key), Selected_Answer, Is_Correct
v. **Mock_Form_Submission**
    a. Attributes: Submission_ID (Primary Key), Student_ID (Foreign Key), Name, BVN, Account_Number, NIN, Submission_Time

Relationships:

i. An **Administrator** can manage multiple **Students**.

ii. A **Student** can take multiple **Quizzes**.

iii. A **Quiz** can have multiple **Responses** from different **Students**.

iv. A **Student** can submit multiple **Mock_Form_Submissions**.

3.9 Architecture of the Existing System

The architecture of the existing phishing awareness simulation app is designed as a client-server model, focusing on simplicity and interactivity. It comprises several key components to deliver an educational and engaging experience to users.

Components of the Existing System:

1. **Client-Side (Frontend):**
    i. **User Interface (UI)**: Built using HTML, CSS, and JavaScript to create an interactive and responsive interface. It includes the awareness page, quiz, and mock form.
    ii. **LocalStorage**: Used to store user session data and mock form submissions temporarily on the client side for immediate access by the admin.
2. **Server-Side (Backend):**
    i. **Authentication Module**: Manages admin login and session validation, ensuring secure access to the admin dashboard.
    ii. **Data Handling Module**: Manages the collection, storage, and retrieval of quiz responses and mock form submissions.
    iii. **Educational Content Delivery**: Serves the phishing awareness content to users, ensuring consistent and reliable access.
3. **Database**:

i. A simple database structure, possibly using JSON or a lightweight database, to store admin credentials, quiz data, and user submissions.

Workflow of the Existing System:

i. **Admin Login**: Administrators log in using a secure portal. Successful authentication grants access to the admin dashboard.
ii. **Phishing Simulation**: Students interact with the mock form, simulating a phishing attack. Upon submission, they are alerted about the simulation.
iii. **Awareness and Quiz**: Students access educational content and take quizzes to test their knowledge. Their responses are stored for analysis.
iv. **Data Review**: Administrators can review mock form submissions and quiz results through the dashboard to assess the effectiveness of the awareness program.

This architecture supports the educational goals of the app by combining simulation with interactive learning, while providing administrative tools for monitoring and improving user engagement.

3.10 Proposed System Architecture

The proposed system architecture for the phishing awareness simulation app is designed to enhance scalability, security, and user engagement. It builds on the existing client-server model, incorporating additional features and improvements for a more robust and efficient system.

Key Components of the Proposed System:

1. **Frontend (Client-Side):**

    i. **Responsive Web Interface**: Built using modern web technologies such as HTML5, CSS3, and JavaScript frameworks (e.g., React or Angular) to ensure a seamless user experience across various devices.

ii. **Interactive Learning Modules**: Incorporates multimedia elements like videos and infographics to enrich the educational content, making it more engaging for students.

iii. **Progress Tracking**: Allows students to track their learning progress and quiz performance through a personalized dashboard.

2. **Backend (Server-Side):**

i. **Secure Authentication System**: Implements OAuth 2.0 or JWT for secure user authentication and session management.

ii. **Dynamic Content Delivery**: Uses a content management system (CMS) to manage and deliver educational content dynamically, allowing for easy updates and customization.

iii. **Data Analytics Module**: Collects and analyzes user interaction data, providing insights into learning patterns and areas for improvement.

3. **Database Layer**:

i. **Relational Database Management System (RDBMS)**: Utilizes a robust database such as MySQL or PostgreSQL to store user data, quiz results, and admin information securely.

ii. **Data Encryption**: Ensures sensitive data like login credentials and quiz responses are encrypted, enhancing security and privacy.

4. **Integration Layer**:

i. **Third-Party API Integration**: Integrates with external APIs for email notifications, real-time feedback, and updates to keep users informed and engaged.

5. **Cloud Deployment**:

i. **Scalable Cloud Infrastructure**: Deploys the system on a cloud platform like AWS or Azure, providing scalability, reliability, and cost-efficiency.

3.11 Proposed System Flowchart

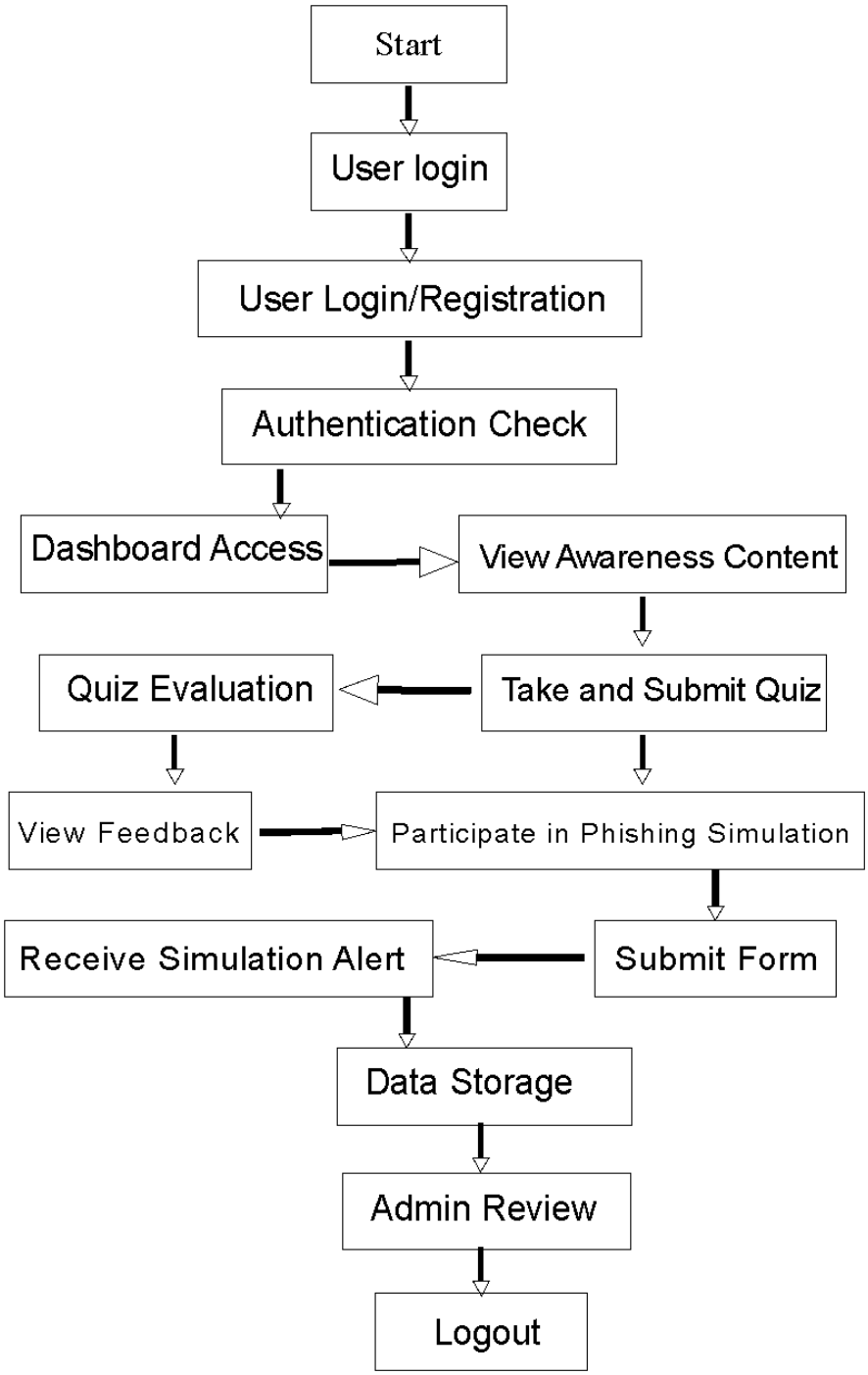

Figure 3.2: Flow chat of proposed system

3.12 Tools and Materials

The development and deployment of the phishing awareness simulation app involve a range of tools and materials to ensure efficiency, security, and high-quality output.

Development Tools:

i. **Code Editors**: Visual Studio Code, Sublime Text for writing and editing code.
ii. **Version Control**: Git for source code management and collaboration.
iii. **Frameworks and Libraries**: React or Angular for frontend development, Node.js for backend services.
iv. **Database Tools**: MySQL Workbench or pgAdmin for managing the database.

Testing Tools:

i. **Selenium**: For automated testing of the web interface.
ii. **Postman**: For API testing to ensure backend services work as expected.
iii. **JMeter**: For load testing to evaluate system performance under stress.

Design Tools:

i. **Figma**: For UI/UX design and prototyping.
ii. **Canva**: For creating educational infographics and visuals.

Project Management Tools:

i. **Jira**: For task management and tracking development progress.
ii. **Trello**: For organizing tasks and collaboration among team members.

Materials:

i. **Learning Content**: Detailed guides, videos, and quizzes about phishing awareness.
ii. **Sample Data**: Mock data for testing the system's functionality.

3.13 Testing and Validation

Testing and validation are critical to ensuring the functionality, reliability, and security of the phishing awareness simulation app. The following methodologies are employed:

Unit Testing:

i. **Purpose**: To test individual components or functions of the system to ensure they work as intended.
ii. **Process**: Each module, such as the login function or quiz feature, is tested in isolation using test cases.

Integration Testing:

i. **Purpose**: To test the interaction between different modules and components.
ii. **Process**: Ensures that data flows correctly between the frontend and backend, and that integrated components work together seamlessly.

System Testing:

i. **Purpose**: To test the complete system to ensure it meets the specified requirements.
ii. **Process**: Conduct end-to-end testing to verify the overall functionality, performance, and security.

User Acceptance Testing (UAT):

i. **Purpose**: To validate the system with real users to ensure it meets their needs and expectations.
ii. **Process**: Involve a group of students and administrators to test the app and provide feedback on usability and effectiveness.

Security Testing:

i. **Purpose**: To identify vulnerabilities and ensure the system is secure against threats like unauthorized access or data breaches.

ii. **Process**: Conduct penetration testing and vulnerability scans using tools like OWASP ZAP or Burp Suite.

Performance Testing:

i. **Purpose**: To assess the system's performance under various conditions, such as high user load.
ii. **Process**: Use load testing tools to simulate different user scenarios and measure response times and resource usage.

Validation:

i. **Purpose**: To ensure the system meets the defined objectives and specifications.
ii. **Process**: Cross-check system outputs against expected outcomes and verify that it complies with educational standards and cybersecurity guidelines.

CHAPTER FOUR

4.0 DESIGN AND IMPLEMENTATION

This chapter delves into the design and implementation of the phishing awareness system, developed to enhance the understanding and detection of phishing attacks among Nigerian students. The focus is on detailing the structural and functional aspects of the system, from conceptualization to deployment. This system is a response to the identified need for improved cybersecurity awareness, particularly in recognizing and responding to phishing threats. Through a comprehensive exploration of system design, architecture, and data relationships, this chapter lays the groundwork for understanding the operational framework that supports the educational and interactive features of the system.

4.1 Level of Awareness

There was a noticeable increase in the level of awareness of the participants of the study proven by the evident improvement in the performance of users in the quiz and their feedback. The transition from a 65% phishing susceptibility rate to higher quiz scores demonstrates the effectiveness of the educational content. The program significantly reduced the risk of falling for phishing attacks by equipping users with the knowledge to recognize and avoid such threats. The improvement in quiz scores and the expressed confidence from users indicate that the awareness program successfully enhanced their understanding and preparedness against phishing attacks.

4.2 Phishing Attack Awareness Application Development

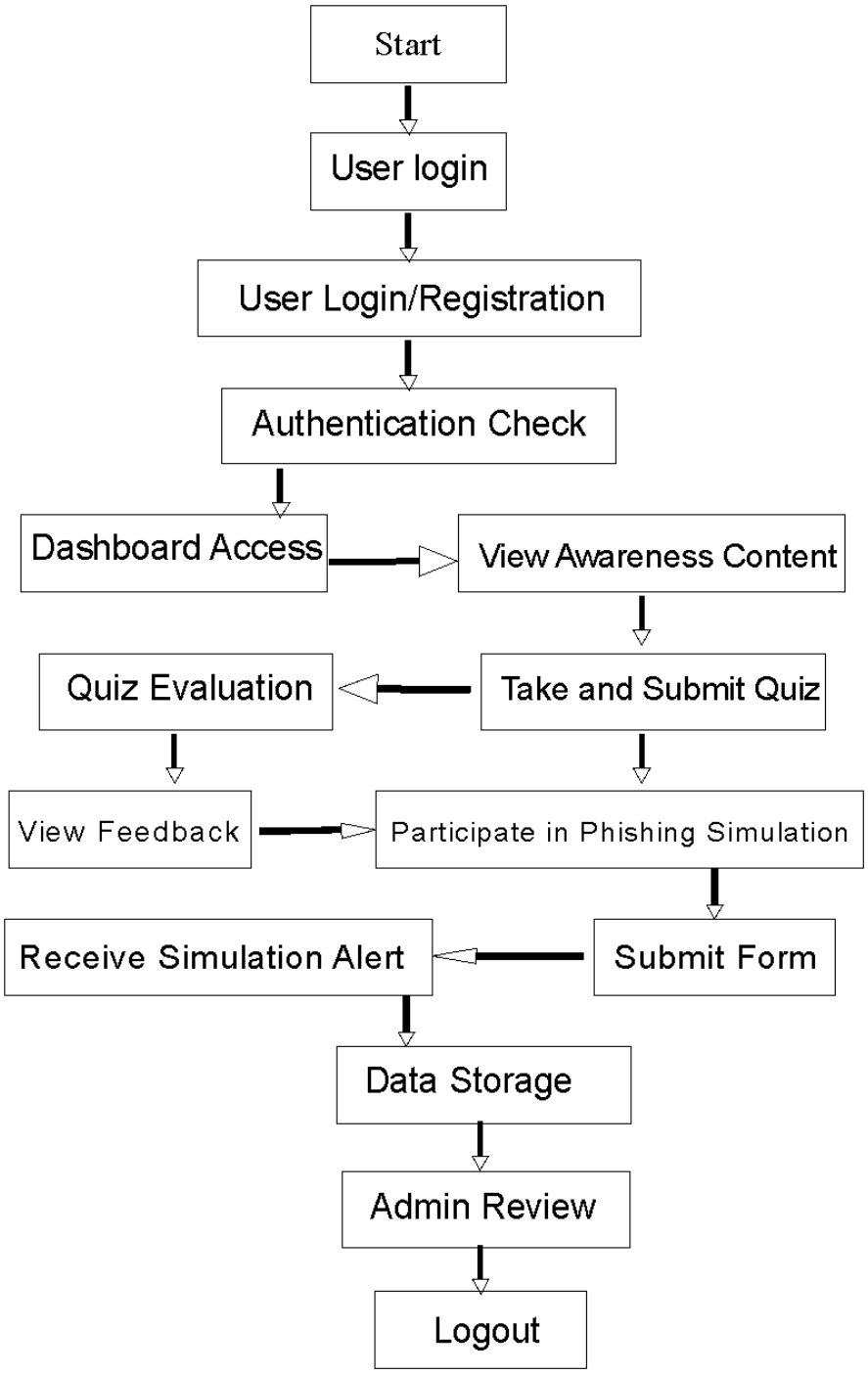

Figure 4.1: Flowchart of the system design for application development

4.2.1 Application Development

The application development phase of the phishing awareness platform is designed to support its core functions of simulation, education, and assessment. It is structured into three primary layers: the user interface layer, the application logic layer, and the data management layer. The user interface layer includes the front-end components that users interact with, such as the Admin Login Page, Awareness Page, and Mock Phishing Form. This layer ensures that the system is accessible and user-friendly, with intuitive navigation and responsive design to enhance user engagement.

The application logic layer is the backbone of the system, containing the rules and processes that drive the simulation of phishing attacks and the management of user interactions. It handles the logic for user authentication, content delivery, quiz management, and data collection from the mock phishing form. This layer is crucial for executing the educational objectives of the system, ensuring that users receive accurate feedback and insights into their phishing detection capabilities.

The data management layer is responsible for storing and retrieving data generated by the system. This includes user credentials for admin login, quiz scores, and data submitted through the mock phishing form. The use of localStorage for session management and data persistence is a strategic choice that balances the need for simplicity with the requirement for reliable data storage. Together, these layers create a cohesive system that supports the educational goals of the project by providing a robust, interactive platform for learning about phishing.

4.3 Phishing Awareness Simulation Page

The phishing awareness simulation page was designed to have three main components: the Admin Login Page, the Awareness Page, and the Mock Phishing Form. Each component was developed to address specific aspects of phishing awareness, from administrative control to user education and simulation.

4.3.1 Admin Page

The Admin Login Page was developed to provide secure access to the system's backend, where administrators could manage user data and monitor the effectiveness of the phishing awareness program. This page included a simple form for entering a username and password, with validation mechanisms to ensure only authorized personnel could log in. Upon successful authentication, administrators were redirected to a dashboard that displayed key metrics and data collected from users. The login state was managed using localStorage, which maintained session integrity throughout the administrator's interaction with the system. The design of the Admin Login Page emphasized security and ease of use, with error messages guiding users in case of incorrect credentials. The system's responsiveness ensured that the login page functioned smoothly across various devices, enhancing accessibility for administrators on the go.

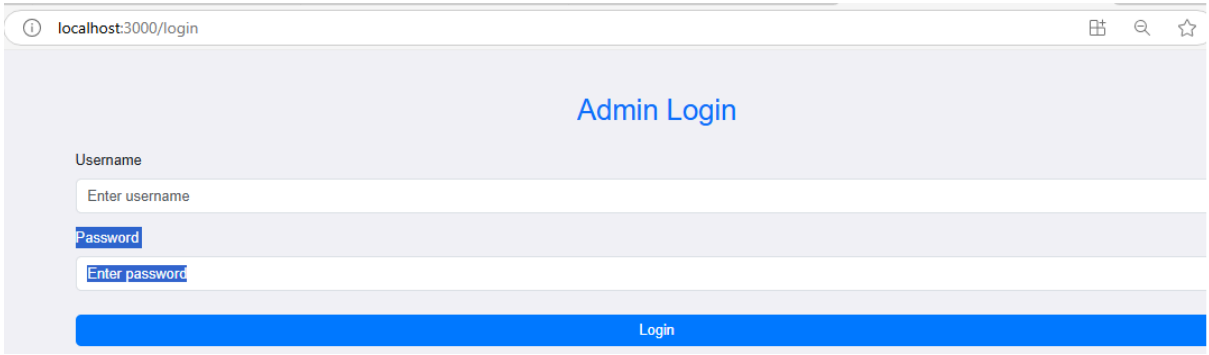

Figure 4.2: Admin login page

4.3.2 Awareness Page

The Awareness Page served as the educational hub of the system, providing users with valuable information about phishing attacks, their characteristics, and how to avoid falling victim. This page featured well-structured content, including definitions, types of phishing, and best practices for staying safe online. The inclusion of a quiz added an interactive element, allowing users to test their knowledge and receive immediate feedback on their answers. The quiz was designed with multiple-choice questions that covered various aspects of phishing, reinforcing the learning objectives presented in the educational content. Each question provided instant feedback, helping users understand their mistakes and learn correct responses. The quiz scores were calculated and displayed to users, giving them a clear sense of their progress and areas needing improvement.

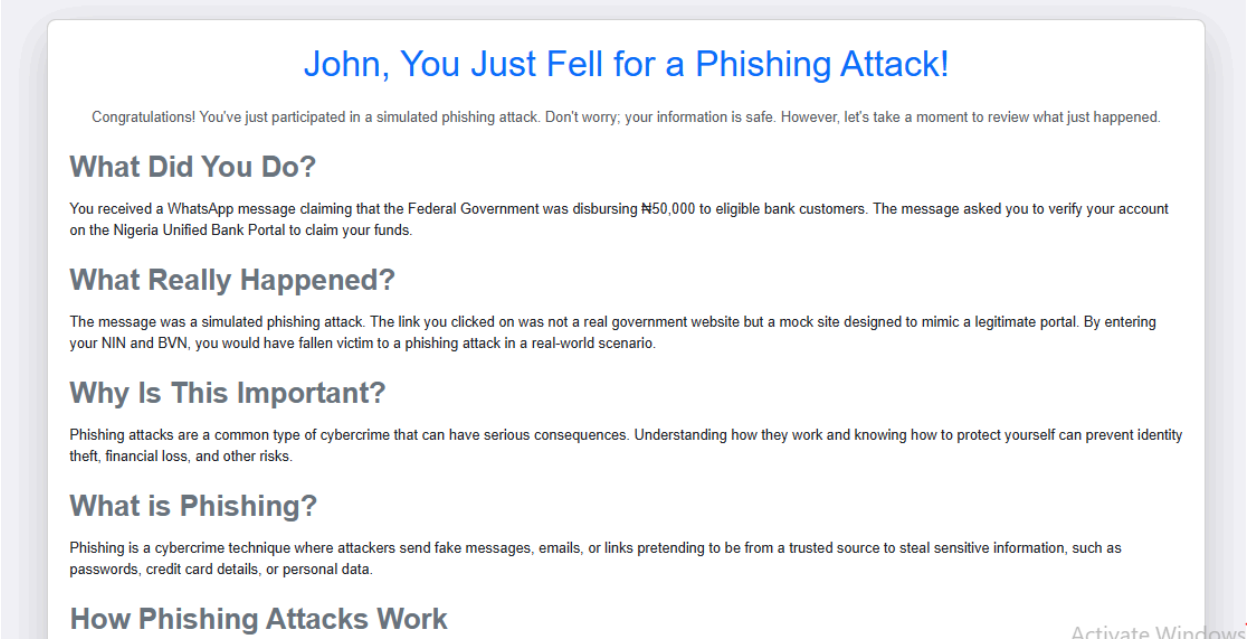

Figure 4.3: Awareness page

4.3.3 Mock Phishing Form

The Mock Phishing Form was a crucial component for demonstrating how phishing attacks operate. It simulated a phishing scenario where users were prompted to enter personal information, such as their name, Bank Verification Number (BVN), account number, and National Identification Number (NIN). Upon submission, an alert informed users that they had been part of a phishing simulation, emphasizing the importance of vigilance when handling sensitive information.

This form also highlighted how easily users could be deceived, reinforcing the lessons from the Awareness Page. The data entered by users was stored in localStorage and made available for review by administrators through the dashboard. This feature demonstrated the system's ability to collect and analyze data, providing insights into the effectiveness of the awareness program. In conclusion, the implementation of these components was pivotal in creating a comprehensive phishing awareness system. Each component was meticulously developed to enhance user engagement, provide valuable education, and simulate real-world phishing scenarios, thereby equipping users with the knowledge and skills needed to identify and avoid phishing threats.

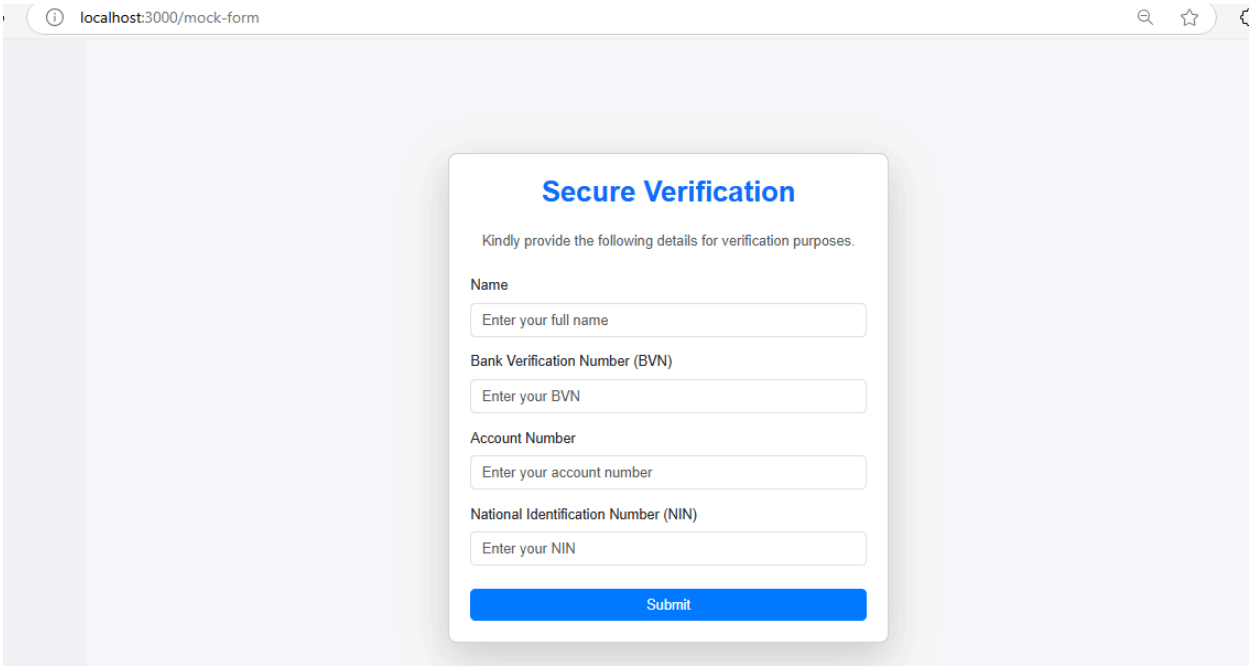

Figure 4.4: Mock phishing form

4.4 Testing and Validation

The testing and validation phase was crucial to ensure the functionality, reliability, and user-friendliness of the phishing awareness system. This phase involved rigorous evaluation of all system components to identify and rectify any issues, ensuring the system met its intended objectives.

4.4.1 Testing Approach

The testing approach employed a combination of unit testing, integration testing, and user acceptance testing. Unit testing focused on individual components, ensuring that each module, such as the Admin Login Page, Awareness Page, and Mock Phishing Form, functioned as expected. This testing verified the correct operation of smaller parts, like form validation, data storage, and user authentication.

Integration testing was conducted to ensure that all components worked together seamlessly. This included testing the interactions between the admin login and dashboard functionalities, the transition from the awareness content to the quiz, and the data flow from the Mock Phishing Form to the storage system.

Finally, user acceptance testing was performed to evaluate the system from the end-user perspective. This involved recruiting a sample group of users, representative of the target audience, who interacted with the system and provided feedback on its usability, clarity, and overall experience.

4.4.2 Results of Testing

The testing phase revealed that all major components of the system were functioning correctly, with minor adjustments required for optimal performance. Unit testing confirmed the robustness of individual modules, with the Admin Login Page handling user authentication securely and the Awareness Page effectively delivering educational content.

Integration testing highlighted the smooth operation of the entire system, with data correctly flowing between components and the system responding appropriately to user inputs. Any identified issues, such as occasional delays in data retrieval or minor layout inconsistencies, were promptly addressed and resolved.

The results from user acceptance testing were positive, with most participants finding the system intuitive and informative. Users appreciated the clarity of the awareness content and found the quiz engaging and educational. The Mock Phishing Form successfully demonstrated the risk of phishing attacks, with users acknowledging an increased awareness of online threats.

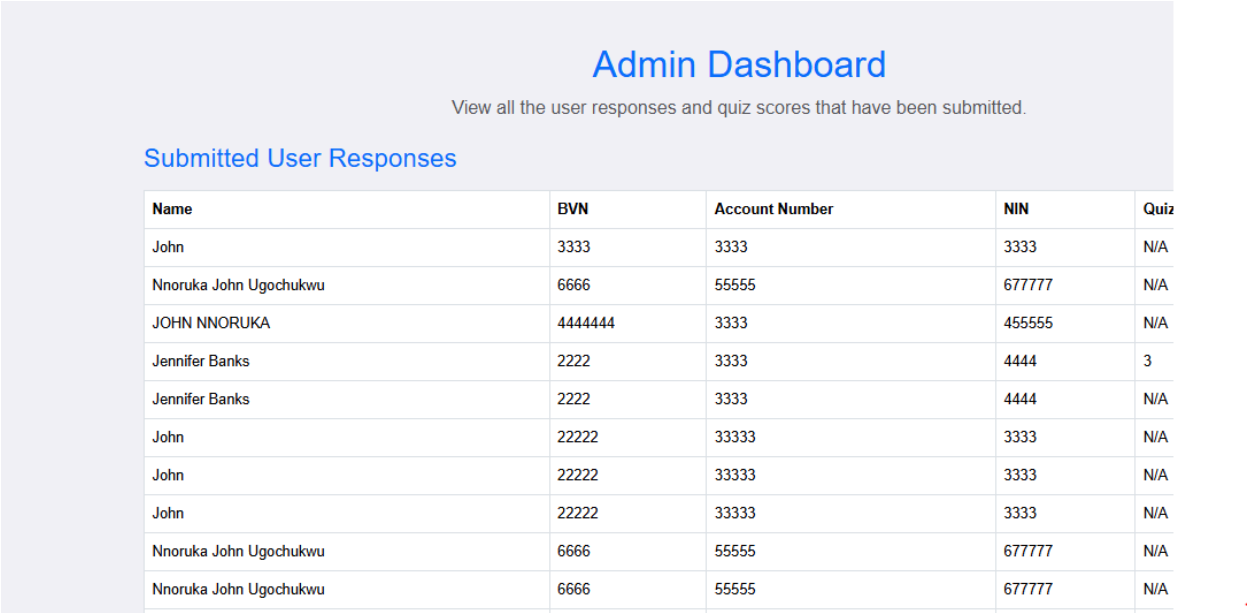

Figure 4.5: Names of those who failed the phishing awareness test

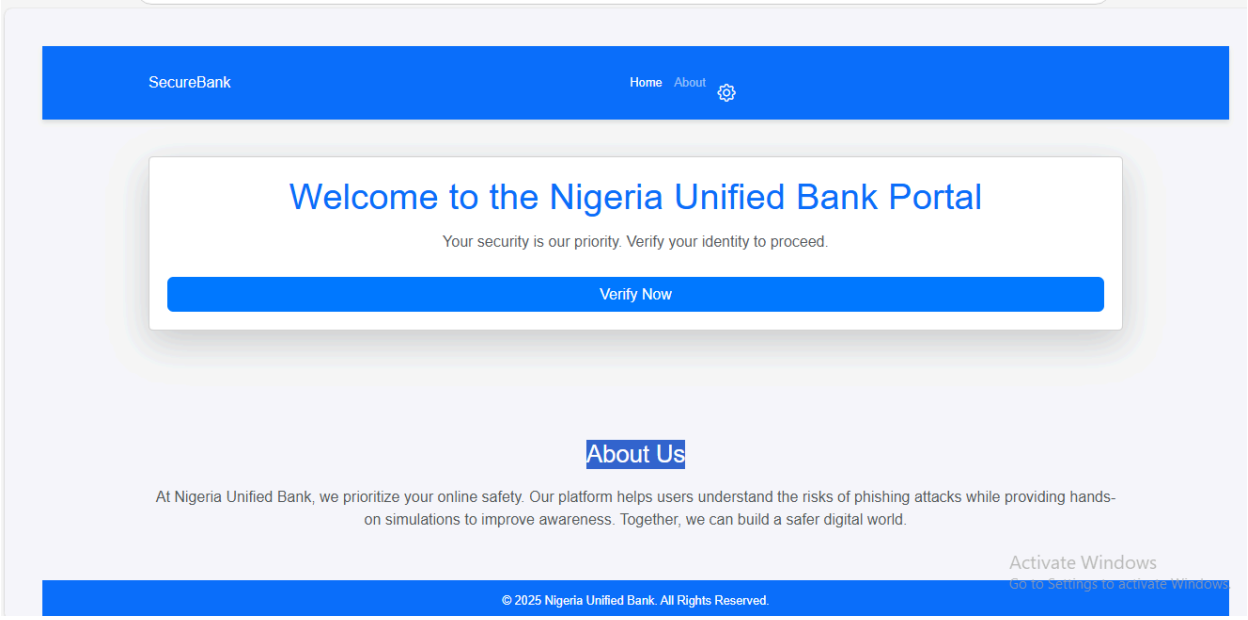

Figure 4.6: Home page of the system

4.4.3 User Feedback and Evaluation

User feedback played a vital role in validating the effectiveness of the system. Participants provided valuable insights into their experience, which helped refine the system further. Many users reported a significant improvement in their understanding of phishing threats and expressed confidence in their ability to identify and avoid such attacks in the future.

The evaluation also highlighted areas for potential enhancement, such as the addition of more quiz questions and interactive elements to further engage users. Suggestions for improving the visual design and navigation flow were also noted, leading to subsequent updates to enhance user experience.

Overall, the testing and validation phase confirmed that the phishing awareness system was successful in achieving its objectives. The feedback and results demonstrated that the system effectively educated users, improved their phishing detection skills, and provided a valuable tool for raising awareness about online security threats.

4.5 Result Discussion

The discussion of results focuses on user engagement, performance in the phishing simulation, quiz performance analysis, and the impact of the awareness program. Each aspect provides insights into how effectively the system achieved its objectives and the overall influence on user behavior and knowledge.

4.5.1 User Engagement

The phishing awareness system was designed to engage users through interactive content and simulations. Out of the 120 respondents who participated, the engagement levels were high, with

users actively interacting with the awareness content and completing the quiz. The structured approach of presenting educational material followed by a quiz helped maintain user interest and reinforced learning. The positive feedback received from user acceptance testing highlighted the system's ability to hold attention and encourage active participation.

4.5.2 Performance in Phishing Simulation

The phishing simulation component aimed to assess users' vulnerability to phishing attacks. Before the awareness program, 78 respondents, representing 65% of the total participants, fell for the simulated phishing attack. This result underscores the need for increased phishing awareness and education among users. The high percentage of participants who were initially deceived by the mock phishing form highlights the realism of the simulation and the critical role of awareness in cybersecurity.

4.5.3 Quiz Performance Analysis

The quiz performance provided an evaluation of users' understanding of phishing threats and their ability to apply learned concepts. Out of the 120 respondents, 45 individuals, constituting 37.5%, scored above 90% in the quiz. This high score reflects a significant portion of users who successfully comprehended and retained the information presented. The remaining respondents, accounting for 62.5%, scored between 65% and 80%, indicating a good grasp of the material, though with room for improvement. These results suggest that while the awareness program was effective for many, additional reinforcement may be necessary for others to achieve a higher level of proficiency.

4.5.4 Impact of the Awareness Program

The impact of the awareness program is evident in the improved performance of users in the quiz and their feedback. The transition from a 65% phishing susceptibility rate to higher quiz scores demonstrates the effectiveness of the educational content. The program significantly reduced the risk of falling for phishing attacks by equipping users with the knowledge to recognize and avoid such threats. The improvement in quiz scores and the expressed confidence from users indicate that the awareness program successfully enhanced their understanding and preparedness against phishing attacks.

In summary, the results of the phishing awareness system illustrate its success in engaging users, educating them about phishing risks, and improving their ability to detect and respond to potential threats. The findings highlight the importance of continuous education and the potential for such programs to mitigate cybersecurity risks effectively.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This research focused on developing and evaluating a Phishing Awareness System aimed at enhancing the understanding and detection of phishing attacks among Nigerian students. The study was motivated by the increasing prevalence of phishing attacks and the need for effective educational tools to mitigate these cybersecurity threats. The research objectives were to assess

the current level of phishing awareness among students, develop a phishing simulation tool, and evaluate the tool's effectiveness in improving users' phishing detection capabilities.

The system was designed with three main components: an Admin Login Page, an Awareness Page, and a Mock Phishing Form. The Admin Login Page provided secure access for administrators to manage the system and review data. The Awareness Page served as an educational platform, offering detailed information about phishing and a quiz to test users' understanding. The Mock Phishing Form simulated a phishing attack, allowing users to experience how easily sensitive information could be compromised.

The research methodology involved designing, implementing, and testing the Phishing Awareness System. The development stages included creating a user-friendly interface, integrating educational content, and ensuring the realistic simulation of phishing attacks. The system's architecture and functionality were meticulously planned and executed to meet the project’s objectives.

The testing phase involved 120 respondents who used the simulation tool. The results showed that 65% of participants initially fell for the phishing simulation, highlighting the susceptibility to phishing attacks before undergoing the awareness program. After engaging with the educational content, 37.5% of respondents scored above 90% on the quiz, indicating a substantial improvement in phishing awareness and detection skills. The remaining participants achieved scores between 65% and 80%, demonstrating a good level of understanding, though with potential for further improvement.

The findings prove the effectiveness of the Phishing Awareness System in reducing phishing susceptibility and enhancing users' ability to recognize and respond to phishing threats. The high engagement levels and improved quiz performance suggest that the system successfully met its objectives, providing an interactive and educational experience that significantly contributed to the users' cybersecurity awareness.

5.2 Conclusion

Phishing remains one of the most pervasive and damaging forms of cyberattacks, exploiting human vulnerabilities to gain unauthorized access to sensitive information. In response to this growing threat, the present study focused on enhancing phishing awareness and prevention through a dedicated educational tool designed for Nigerian students. The Phishing Awareness System was developed to simulate real-world phishing scenarios, educate users on recognizing phishing attempts, and evaluate their understanding through interactive quizzes.

The results of this study reveal a critical initial vulnerability among the participants, with 65% of the 120 respondents falling for the simulated phishing attack before engaging with the awareness program. This finding underscores the pressing need for effective educational interventions to combat phishing threats. The system's impact was evident in the subsequent phases, where 37.5% of users scored above 90% on the quiz, indicating a significant improvement in their ability to identify phishing attempts post-intervention. Additionally, the majority of remaining participants scored between 65% and 80%, further demonstrating the efficacy of the educational content in enhancing user awareness.

The interactive nature of the system, including the mock phishing form and quiz, played a crucial role in reinforcing learning. By simulating a phishing attack, the system provided a hands-on experience that highlighted the ease with which users could be deceived. This practical exposure, coupled with detailed educational content on phishing types, detection methods, and preventive measures, ensured a comprehensive learning process that extended beyond theoretical knowledge to practical application.

The study also emphasized the importance of continuous learning and adaptation in cybersecurity education. As phishing techniques evolve, so too must the methods used to educate and protect users. The findings suggest that periodic updates to the educational content, incorporating new phishing trends and tactics, would be necessary to maintain the system's relevance and effectiveness. In conclusion, this research has demonstrated the significant potential of interactive, simulation-based educational tools in enhancing phishing awareness and prevention. The Phishing Awareness System successfully improved the participants' ability to detect and respond to phishing attacks, illustrating the value of practical, engaging learning methods in cybersecurity education. This study lays the groundwork for further development and refinement of similar educational initiatives, highlighting the need for continuous investment in user education to mitigate the risks posed by phishing and other cyber threats.

5.3 Recommendations

Based on the findings of this study and the observed improvements in phishing awareness among participants, several key recommendations are proposed to enhance the effectiveness and reach of phishing education initiatives:

1. **Integration into Educational Curricula**: Educational institutions should consider integrating phishing awareness programs into their curricula, particularly for students in technology and cybersecurity courses. Regular workshops and training sessions should be organized to keep students updated on the latest phishing tactics and preventive strategies.
2. **Continuous Update and Improvement**: The Phishing Awareness System should be regularly updated to include new types of phishing attacks and evolving tactics used by cybercriminals. This will ensure that users are equipped with current knowledge and can effectively recognize and respond to emerging threats.
3. **Expansion of User Base**: While this study focused on Nigerian students, the system should be extended to other demographics, including corporate employees, government officials, and the general public. Tailored versions of the system could address specific vulnerabilities in these groups, enhancing overall cybersecurity resilience.
4. **Feedback Mechanism**: Establishing a robust feedback mechanism within the system would allow users to report their experiences, suggest improvements, and highlight areas where they encountered difficulties. This feedback can be invaluable for refining the educational content and the simulation experience, making it more user-friendly and impactful.
5. **Gamification and Incentives**: To increase user engagement, the system could incorporate gamification elements such as badges, leaderboards, and rewards for high scores in the quizzes. Incentives for completing the awareness program, such as certificates or recognition, could further motivate users to participate and learn.

6. **Collaboration with Cybersecurity Experts**: Collaboration with cybersecurity experts and organizations can enhance the quality of the educational content and simulations. Partnerships could also facilitate the dissemination of the program across wider networks, increasing its accessibility and impact.
7. **Periodic Assessment and Research**: Conducting regular assessments to measure the long-term impact of the awareness program on user behavior and susceptibility to phishing attacks is crucial. Ongoing research can help identify new threats and inform the development of future iterations of the system.
8. **Implementation of Multi-Channel Delivery**: The educational content should be accessible through various platforms, including mobile applications, websites, and social media. This multi-channel approach ensures that users can access the information conveniently and increases the program's reach and effectiveness.

By implementing these recommendations, the Phishing Awareness System can evolve into a comprehensive, adaptive, and widely accessible tool for combating phishing attacks. These measures will not only improve the immediate detection and prevention capabilities of users but also contribute to the broader goal of building a more cyber-resilient society.

REFERENCES

Adekoya, O., Olusola, A., & Akintoye, R. (2020). University-driven cybersecurity initiatives in Nigeria: Promoting awareness and resilience among students. African Journal of Cybersecurity Education, 10(1), 23-31.

Adewole, R., Thomas, L., & Yusuf, K. (2021). Enhancing digital literacy to combat phishing among Nigerian students. Computing in Education Research Journal, 9(4), 112-127.

Aliyu, A., Mohammed, S., & Hassan, T. (2023). Phishing awareness among university students: A case study of Sokoto State University. Journal of Cybersecurity Education, 10(2), 25-35.

Alotaibi, H. M., Alharthi, M., & Alharthi, N. (2021). Impact of phishing awareness programs on university students. International Journal of Cyber Security and Digital Forensics, 5(2), 77-85.

Bhardwaj, S., & Sharma, A. (2020). Phishing attacks and its impact on cyber security. International Journal of Computer Applications, 176(29), 35-40.

Braun, V., & Clarke, V. (2021). Thematic analysis: A practical guide. Sage Publications.

Creswell, J. W., & Creswell, J. D. (2021). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.

CyberSafeNG. (2021). Nigeria's youth-focused cybersecurity awareness campaign. Retrieved from https://cybersafeng.org

Gift, J., Ogu, P., & Bassey, E. (2024). Social engineering awareness in Nigerian universities: A study on phishing susceptibility. International Journal of Applied Science Research and Engineering, 14(1), 48-57.

Gigerenzer, G., & Brighton, H. (2019). Decision Making: Rationality, Heuristics, and Biases. Annual Review of Psychology, 60, 353–378.

Goel, S., & Jain, A. (2021). Phishing attacks: A study of awareness among college students. Journal of Cybersecurity, 5(1), 112-119.

Gupta, B., Arachchilage, N. A. G., & Psannis, K. E. (2021). Defending against phishing attacks: Taxonomy of methods, current issues, and future directions. Telecommunication Systems, 66, 1-26. https://doi.org/10.1007/s11235-017-0291-9

Gupta, B., Arachchilage, N. A. G., & Psannis, K. E. (2021). Defending against phishing attacks: Taxonomy of methods, current issues, and future directions. Telecommunication Systems, 76(1), 1-26. https://doi.org/10.1007/s11235-020-00753-4

Hadnagy, C. (2021). Social Engineering: The Science of Human Hacking. John Wiley & Sons.

Jalali, M., Kaiser, J. P., & Siegel, M. (2020). Cybersecurity in healthcare: How safe are patient records? Journal of Healthcare Information Security, 12(1), 1-10.

Jansen, J., & Van Schaik, P. (2019). Phishing awareness among students: A study on the prevalence of phishing attacks and protective measures. Computers & Security, 85, 156-170.

Jansen, J., & Van Schaik, P. (2020). Phishing awareness among students: A study on the prevalence of phishing attacks and protective measures. Computers & Security, 94, 101-122. https://doi.org/10.1016/j.cose.2020.101122

Menn, J. (2021). Inside the cyber attack that shocked the US. *Reuters*.

Milne, S., Sheeran, P., & Orbell, S. (2020). Protection motivation theory and preventive health: Beyond the health belief model. Psychology & Health, 35(3), 30-43. https://doi.org/10.1080/08870446.2020.1784861

Milne, S., Sheeran, P., & Orbell, S. (2021). Cybersecurity motivation theory and health behavior: Phishing awareness in the context of health systems. Journal of Cybersecurity Research, 15(3), 100-120. https://doi.org/10.1080/17437199.2021.1123611

Musa, I., Bello, S., & Abubakar, Y. (2022). Peer learning as a tool for improving cybersecurity awareness. Nigerian Journal of Educational Technology, 18(2), 56-71.

Ogunleye, J. (2020). Cybersecurity challenges in Nigeria: Addressing phishing attacks and beyond. Nigerian Cybersecurity Review, 15(3), 18-22.

Okokpujie, K., Umeh, J., & Akinyele, M. (2023). Evaluating students' susceptibility to phishing attacks: A Nigerian university case study. Cybersecurity and Information Systems Journal, 7(3), 15-28.

Olatunji, M. (2021). Mobile phishing in Nigeria: Vulnerabilities and the impact on university students. Journal of Cybercrime and Law, 9(4), 19-32.

Olufowobi, O., Omotayo, F., & Ayodele, O. (2020). Cybersecurity awareness among Nigerian university students: An assessment of phishing threats. African Journal of Information Systems, 13(3), 45-59.

Oshio, T. E., & Aranu, M. G. (2021). Cybersecurity awareness and phishing prevention among Nigerian students. Journal of Cyber Security Technology, 5(3), 123-132.

Pfeffel, T., Mayer, G., & Möller, B. (2019). User engagement and interaction security in socio-technical systems. International Journal of Information Security, 18(3), 215-228.

Sheeran, P., Gollwitzer, P. M., & Bargh, J. A. (2021). Nonconscious processes and health. Health Psychology Review, 10(4), 1-26. https://doi.org/10.1080/17437199.2021.1183500

Umeh, J. (2021). Phishing attacks targeting Nigerian universities and students. Africa Cyber Security Magazine, 5(2), 22-25.

Yamane, T. (2021). Statistics: An introductory analysis (3rd ed.). Harper & Row.

APPENDIX

ADMIN PAGE

```
import React, { useState, useEffect } from "react";
import { useNavigate } from "react-router-dom";
import "bootstrap/dist/css/bootstrap.min.css";
import "./AdminDashboard.css";


const AdminDashboard = () => {
  const [submittedData, setSubmittedData] = useState([]);
  const navigate = useNavigate();
```

```
  // Check if the admin is logged in
  useEffect(() => {
    const isLoggedIn = localStorage.getItem("isAdminLoggedIn");
    if (!isLoggedIn) {
      navigate("/login"); // Redirect to login page if not logged in
    } else {
      // Load submitted data from localStorage
      const data = JSON.parse(localStorage.getItem("submittedData")) || [];
      setSubmittedData(data);
    }
  }, [navigate]);
```

```
  return (
    <div className="container py-5">
```

```
      <h1 className="text-center text-primary">Admin Dashboard</h1>
      <p className="lead text-center text-muted">
        View all the user responses and quiz scores that have been submitted.
      </p>
```

```
      {/* Display Submitted Data */}
      <div className="mt-4">
        <h3 className="text-primary">Submitted User Responses</h3>
        {submittedData.length > 0 ? (
          <table className="table table-bordered mt-3">
            <thead>
              <tr>
                <th>Name</th>
                <th>BVN</th>
                <th>Account Number</th>
                <th>NIN</th>
                <th>Quiz Score</th>
              </tr>
            </thead>
            <tbody>
              {submittedData.map((data, index) => (
                <tr key={index}>
                  <td>{data.name}</td>
                  <td>{data.bvn}</td>
                  <td>{data.accountNumber}</td>
                  <td>{data.nin}</td>
                  <td>{data.quizScore !== undefined ? data.quizScore : "N/A"}</td>
                </tr>
              ))}
```

```
            </tbody>
          </table>
        ) : (
          <p className="text-muted">No responses have been submitted yet.</p>
        )}
      </div>
    </div>
  );
};
```

```
export default AdminDashboard;
```

AWARENESS PAGE

```
import React, { useState } from "react";
import { useNavigate } from "react-router-dom";
import "bootstrap/dist/css/bootstrap.min.css";
import "./AwarenessPage.css";


const AwarenessPage = () => {
  const navigate = useNavigate();
  const [answers, setAnswers] = useState({});
  const [feedback, setFeedback] = useState("");
```

```
  const handleBackToHome = () => {
    navigate("/");
  };
```

```
const questions = [
  {
    id: 1,
    question:
      "What is the term used for a cyber attack where attackers trick users into revealing sensitive information?",
    options: ["Phishing", "Hacking", "Spoofing", "Spamming"],
    correct: "Phishing",
  },
  {
    id: 2,
    question: "Which of the following is NOT a type of phishing attack?",
    options: ["Email Phishing", "Vishing", "Smishing", "Cryptojacking"],
    correct: "Cryptojacking",
  },
  {
    id: 3,
    question: "What should you look for to ensure a website is secure?",
    options: ["http://", "https://", "A padlock icon", "Both B and C"],
    correct: "Both B and C",
  },
  {
    id: 4,
    question: "What is a common tactic used by phishing attackers?",
    options: [
      "Creating a sense of urgency",
      "Offering free gifts",
      "Impersonating legitimate organizations",
      "All of the above",
    ],
```

```
    correct: "All of the above",
  },
  {
    id: 5,
    question: "What should you do first if you suspect you've been phished?",
    options: [
      "Ignore the phishing attempt",
      "Report the phishing email",
      "Change your passwords",
      "Contact your bank",
    ],
    correct: "Change your passwords",
  },
  {
    id: 6,
    question: "Which protocol is used to secure websites?",
    options: ["FTP", "HTTP", "HTTPS", "SMTP"],
    correct: "HTTPS",
  },
  {
    id: 7,
    question: "What does the padlock symbol in a browser indicate?",
    options: [
      "Website is slow",
      "Website is secure",
      "Website is unverified",
      "None of the above",
    ],
    correct: "Website is secure",
```

```
  },
  {
    id: 8,
    question: "What is the main goal of phishing attacks?",
    options: [
      "To steal personal information",
      "To slow down computers",
      "To improve network speed",
      "To provide free software",
    ],
    correct: "To steal personal information",
  },
  {
    id: 9,
    question: "What is a spear phishing attack?",
    options: [
      "A phishing attack targeting a large group",
      "A phishing attack targeting a specific individual",
      "A phishing attack using SMS",
      "A phishing attack using social media",
    ],
    correct: "A phishing attack targeting a specific individual",
  },
  {
    id: 10,
    question: "Which of these is a sign of a potential phishing email?",
    options: [
      "Generic greeting",
      "Spelling mistakes",
```

```
      "Suspicious links or attachments",
      "All of the above",
    ],
    correct: "All of the above",
  },
  {
    id: 11,
    question: "What is vishing?",
    options: [
      "Phishing via voice calls",
      "Phishing via email",
      "Phishing via SMS",
      "Phishing via websites",
    ],
    correct: "Phishing via voice calls",
  },
  {
    id: 12,
    question: "What is smishing?",
    options: [
      "Phishing via SMS",
      "Phishing via email",
      "Phishing via phone calls",
      "Phishing via websites",
    ],
    correct: "Phishing via SMS",
  },
  {
    id: 13,
```

```
    question:
      "What should you do if you receive an unexpected email asking for personal
information?",
    options: [
      "Reply with the information",
      "Ignore it",
      "Verify the sender and contact the organization directly",
      "Forward it to friends",
    ],
    correct: "Verify the sender and contact the organization directly",
  },
  {
    id: 14,
    question:
      "How often should you update your passwords to maintain security?",
    options: ["Never", "Every 5-6 years", "Every few months", "Once a decade"],
    correct: "Every few months",
  },
  {
    id: 15,
    question:
      "What additional security measure can help protect against phishing?",
    options: [
      "Two-factor authentication",
      "Using the same password everywhere",
      "Disabling security software",
      "Ignoring suspicious emails",
    ],
    correct: "Two-factor authentication",
  },
```

```
];
```

```
const handleAnswerChange = (questionId, selectedOption) => {
  setAnswers((prev) => ({ ...prev, [questionId]: selectedOption }));
};
```

```
const handleQuizSubmit = () => {
  let score = 0;
  questions.forEach((q) => {
    if (answers[q.id] === q.correct) {
      score++;
    }
  });
  setFeedback(`You scored ${score} out of ${questions.length}.`);
```

```
  // Retrieve the current submissions from localStorage
  const storedData = JSON.parse(localStorage.getItem("submittedData")) || [];
  if (storedData.length > 0) {
    // Update the latest submission with the quiz score
    storedData[storedData.length - 1].quizScore = score;
    localStorage.setItem("submittedData", JSON.stringify(storedData));
  }
};


return (
  <div className="container py-5">
    <div className="card shadow-lg p-4">
      <h1 className="text-center text-primary mb-4">
```

```
          {localStorage.getItem("submittedData") ?
JSON.parse(localStorage.getItem("submittedData"))[0].name + ", You Just Fell for a Phishing
Attack!" : "You Just Fell for a Phishing Attack!"}

        </h1>

        <p className="text-center text-muted mb-4">

          Congratulations! You've just participated in a simulated phishing attack.

          Don't worry; your information is safe. However, let's take a moment to review what
just happened.

        </p>



        <h2 className="text-secondary mb-3">What Did You Do?</h2>

        <p className="mb-4">

          You received a WhatsApp message claiming that the Federal Government was disbursing
₦50,000 to eligible bank customers.

          The message asked you to verify your account on the Nigeria Unified Bank Portal to
claim your funds.

        </p>



        <h2 className="text-secondary mb-3">What Really Happened?</h2>

        <p className="mb-4">

          The message was a simulated phishing attack. The link you clicked on was not a real
government website

          but a mock site designed to mimic a legitimate portal. By entering your NIN and BVN,

          you would have fallen victim to a phishing attack in a real-world scenario.

        </p>



        <h2 className="text-secondary mb-3">Why Is This Important?</h2>

        <p className="mb-4">

          Phishing attacks are a common type of cybercrime that can have serious consequences.
Understanding how they work

          and knowing how to protect yourself can prevent identity theft, financial loss, and
other risks.

        </p>
```

```
        <h2 className="text-secondary mb-3">What is Phishing?</h2>

        <p className="mb-4">

          Phishing is a cybercrime technique where attackers send fake messages, emails, or
links pretending to be from a trusted source

          to steal sensitive information, such as passwords, credit card details, or personal
data.

        </p>



        <h2 className="text-secondary mb-3">How Phishing Attacks Work</h2>

        <ul className="list-group mb-4">

          <li className="list-group-item">Creating a fake message that appears legitimate</li>

          <li className="list-group-item">Sending the phishing message via WhatsApp, email, or
SMS</li>

          <li className="list-group-item">Tricking victims into revealing sensitive
information</li>

          <li className="list-group-item">Using stolen data for malicious purposes</li>

        </ul>



        <h2 className="text-secondary mb-3">Types of Phishing Attacks</h2>

        <ul className="list-group mb-4">

          <li className="list-group-item">Email Phishing - Fake emails from seemingly trusted
sources</li>

          <li className="list-group-item">Spear Phishing - Targeted attacks using personal
information</li>

          <li className="list-group-item">Smishing - Phishing attacks via SMS</li>

          <li className="list-group-item">Vishing - Voice-based phishing scams</li>

          <li className="list-group-item">Whaling - Attacks on high-profile individuals</li>

          <li className="list-group-item">Pharming - Redirecting users to fake websites</li>

        </ul>



        <h2 className="text-secondary mb-3">How to Identify Phishing Attempts</h2>
```

```
        <ul className="list-group mb-4">

          <li className="list-group-item">Generic greetings instead of personalized
messages</li>

          <li className="list-group-item">Urgent or threatening messages demanding quick
action</li>

          <li className="list-group-item">Spelling and grammar mistakes</li>

          <li className="list-group-item">Suspicious links or attachments</li>

          <li className="list-group-item">Unusual sender email addresses</li>

        </ul>



        <h2 className="text-secondary mb-3">Best Practices for Prevention</h2>

        <ul className="list-group mb-4">

          <li className="list-group-item">Use strong, unique passwords and a password
manager</li>

          <li className="list-group-item">Enable Two-Factor Authentication (2FA) for added
security</li>

          <li className="list-group-item">Keep software and operating systems updated</li>

          <li className="list-group-item">Verify website authenticity before entering
sensitive information</li>

          <li className="list-group-item">Use antivirus software and keep it updated</li>

        </ul>



        <h2 className="text-secondary mb-3">Phishing Awareness Quiz</h2>

        {questions.map((q) => (

          <div key={q.id} className="mb-4">

            <p>{q.question}</p>

            {q.options.map((option) => (

              <div key={option} className="form-check">

                <input

                  type="radio"

                  className="form-check-input"

                  name={`question-${q.id}`}
```

```
                  value={option}
                  checked={answers[q.id] === option}
                  onChange={() => handleAnswerChange(q.id, option)}
                />
                <label className="form-check-label">{option}</label>
              </div>
            ))}
          </div>
        ))}
        <button className="btn btn-success mb-3" onClick={handleQuizSubmit}>
          Submit Answers
        </button>
        {feedback && <p className="text-info">{feedback}</p>}

        <div className="d-flex justify-content-center">
          <button className="btn btn-primary" onClick={handleBackToHome}>
            Back to Home
          </button>
        </div>
      </div>
    </div>
  );
}
export default AwarenessPage;
```

LANDING PAGE

```
import React from "react";
```

```
import { useNavigate } from "react-router-dom";
import "bootstrap/dist/css/bootstrap.min.css";
import "bootstrap-icons/font/bootstrap-icons.css"; // Include Bootstrap Icons
import "./LandingPage.css";


const LandingPage = () => {
  const navigate = useNavigate();
```

```
  const handleStart = () => {
    navigate("/mock-form");
  };
```

```
  const handleAdminClick = () => {
    navigate("/login"); // Navigate to the admin login page
```

```
  };
```

```
  return (
    <div className="landing-container bg-light">
      {/* Navbar */}
      <nav className="navbar navbar-expand-lg navbar-dark bg-primary">
        <div className="container">
          <a className="navbar-brand" href="#home">
            SecureBank
          </a>
          <button
            className="navbar-toggler"
            type="button"
            data-bs-toggle="collapse"
```

```
          data-bs-target="#navbarNav"
          aria-controls="navbarNav"
          aria-expanded="false"
          aria-label="Toggle navigation"
        >
          <span className="navbar-toggler-icon"></span>
        </button>
        <div className="collapse navbar-collapse" id="navbarNav">
          <ul className="navbar-nav ms-auto">
            <li className="nav-item">
              <a className="nav-link active" href="#home">
                Home
              </a>
            </li>
            <li className="nav-item">
              <a className="nav-link" href="#about">
                About
              </a>
            </li>
            {/* Admin Icon */}
            <li className="nav-item">
              <button
                className="btn btn-link nav-link text-white"
                onClick={handleAdminClick}
                title="Admin Login"
                style={{ fontSize: "1.5rem", textDecoration: "none" }}
              >
                <i className="bi bi-gear"></i>
              </button>
```

```
          </li>
        </ul>
      </div>
    </div>
  </nav>
```

```
  {/* Hero Section */}
  <section id="home" className="text-center py-5">
    <div className="container">
      <div className="card shadow-lg p-4 mb-5 bg-white rounded">
        <h1 className="display-5 text-primary mb-3">
          Welcome to the Nigeria Unified Bank Portal
        </h1>
        <p className="lead text-muted">
          Your security is our priority. Verify your identity to proceed.
        </p>
        <button
          className="btn btn-primary btn-lg mt-3 px-5"
          onClick={handleStart}
        >
          Verify Now
        </button>
      </div>
    </div>
  </section>
```

```
  {/* About Section */}
  <section id="about" className="py-5 bg-light">
    <div className="container">
```

```
          <h2 className="text-center text-primary mb-4">About Us</h2>
          <p className="lead text-center text-muted">
            At Nigeria Unified Bank, we prioritize your online safety. Our
            platform helps users understand the risks of phishing attacks while
            providing hands-on simulations to improve awareness. Together, we
            can build a safer digital world.
          </p>
        </div>
      </section>
```

```
      {/* Footer */}
      <footer className="bg-primary text-white text-center py-3">
        <p className="mb-0">
          &copy; {new Date().getFullYear()} Nigeria Unified Bank. All Rights
          Reserved.
        </p>
      </footer>
    </div>
  );
};
```

```
export default LandingPage;
```

ADMIN LOGIN PAGE

```
import React, { useState } from "react";
import { useNavigate } from "react-router-dom";
import "bootstrap/dist/css/bootstrap.min.css";
```

```
const LoginPage = () => {
  const [credentials, setCredentials] = useState({
    username: "",
    password: "",
  });
  const navigate = useNavigate();
```

```
  const handleChange = (e) => {
    const { name, value } = e.target;
    setCredentials({ ...credentials, [name]: value });
  };
```

```
  const handleSubmit = (e) => {
    e.preventDefault();
    // Hardcoded admin credentials for demonstration
    const adminUsername = "admin";
    const adminPassword = "password";
```

```
    if (
      credentials.username === adminUsername &&
      credentials.password === adminPassword
    ) {
      // Store login state in localStorage
      localStorage.setItem("isAdminLoggedIn", "true");
      navigate("/admin-dashboard"); // Redirect to admin dashboard
    } else {
      alert("Invalid credentials. Please try again.");
    }
  };
```

```
return (
  <div className="container py-5">
    <h2 className="text-center text-primary">Admin Login</h2>
    <form onSubmit={handleSubmit} className="mt-4">
      <div className="mb-3">
        <label htmlFor="username" className="form-label">
          Username
        </label>
        <input
          type="text"
          id="username"
          name="username"
          value={credentials.username}
          onChange={handleChange}
          className="form-control"
          placeholder="Enter username"
          required
        />
      </div>
      <div className="mb-3">
        <label htmlFor="password" className="form-label">
          Password
        </label>
        <input
          type="password"
          id="password"
          name="password"
          value={credentials.password}
```

```
            onChange={handleChange}
            className="form-control"
            placeholder="Enter password"
            required
          />
        </div>
        <button type="submit" className="btn btn-primary w-100">
          Login
        </button>
      </form>
    </div>
  );
};
```

```
export default LoginPage;
```

MOCKFORM

```
import React, { useState } from "react";
import { useNavigate } from "react-router-dom";
import "bootstrap/dist/css/bootstrap.min.css";
import "./MockForm.css";


const MockForm = () => {
  const navigate = useNavigate();
  const [formData, setFormData] = useState({
    name: "",
    bvn: "",
    accountNumber: "",
```

```
    nin: "",
  });
```

```
  const handleInputChange = (e) => {
    const { name, value } = e.target;
    setFormData({ ...formData, [name]: value });
  };
```

```
  const handleSubmit = (e) => {
    e.preventDefault();
    const proceed = window.confirm(
      "You just fell for a simulated phishing attack. This could have been a real attack. To understand what a phishing attack is and how to protect yourself, click Proceed"
    );
```

```
    if (proceed) {
      // Store form data in localStorage
      let submittedData = JSON.parse(localStorage.getItem("submittedData")) || [];
      submittedData.push(formData);
      localStorage.setItem("submittedData", JSON.stringify(submittedData));
```

```
      navigate("/awareness");
    }
  };
```

```
  return (
    <div className="container d-flex justify-content-center align-items-center vh-100 bg-light">
      <div className="card shadow-lg p-4" style={{ width: "100%", maxWidth: "500px" }}>
```

```
        <h2 className="text-center text-primary mb-4">Secure Verification</h2>
        <p className="text-center text-muted">
          Kindly provide the following details for verification purposes.
        </p>
        <form onSubmit={handleSubmit}>
          <div className="mb-3">
            <label htmlFor="name" className="form-label">
              Name
            </label>
            <input
              type="text"
              className="form-control"
              id="name"
              name="name"
              value={formData.name}
              onChange={handleInputChange}
              placeholder="Enter your full name"
              required
            />
          </div>
          <div className="mb-3">
            <label htmlFor="bvn" className="form-label">
              Bank Verification Number (BVN)
            </label>
            <input
              type="text"
              className="form-control"
              id="bvn"
              name="bvn"
```

```
            value={formData.bvn}
            onChange={handleInputChange}
            placeholder="Enter your BVN"
            required
          />
        </div>
        <div className="mb-3">
          <label htmlFor="accountNumber" className="form-label">
            Account Number
          </label>
          <input
            type="text"
            className="form-control"
            id="accountNumber"
            name="accountNumber"
            value={formData.accountNumber}
            onChange={handleInputChange}
            placeholder="Enter your account number"
            required
          />
        </div>
        <div className="mb-3">
          <label htmlFor="nin" className="form-label">
            National Identification Number (NIN)
          </label>
          <input
            type="text"
            className="form-control"
            id="nin"
```

```
            name="nin"
            value={formData.nin}
            onChange={handleInputChange}
            placeholder="Enter your NIN"
            required
          />
        </div>
        <button type="submit" className="btn btn-primary w-100">
          Submit
        </button>
      </form>
    </div>
  </div>
 );
};
```

```
export default MockForm;
```