PHISHING ATTACKS: A STUDY ON TECHNIQUES AND PREVENTION STRATEGIES AMONG INTERNET USERS

BY

ESOSA DIVINE ENOBAKHARE

PSC2105328

DEPARTMENT OF COMPUTER SCIENCE,
FACULTY OF PHYSICAL SCIENCES,
UNIVERSITY OF BENIN,
BENIN CITY.

NOVEMBER, 2025.

PHISHING ATTACKS: A STUDY ON TECHNIQUES AND PREVENTION STRATEGIES AMONG INTERNET USERS

BY

ESOSA DIVINE ENOBAKHARE

PSC2105328

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

NOVEMBER, 2025.

CERTIFICATION

This is to certify that this research work was carried out by **ESOSA DIVINE ENOBAKHARE** with matriculation number **PSC2105328**, Faculty of Physical Sciences, Department of Computer Science, University of Benin, Benin City under my supervision.

_____

_____

Dr. Mrs. Grace Aziken **Date**

(Project Supervisor)

APPROVAL

This project report written by **ESOSA DIVINE ENOBAKHARE** with matriculation number **PSC2105328** in partial fulfillment of the requirements for the award of the University of Benin Bachelor of Science (BSc) degree in Computer Science, is adequate both in scope and content and it is hereby approved for presentation.

_____

_____

Dr. (Mrs.) A. R. Usiobaifo **Date**

DEDICATION

This project work is dedicated to God Almighty, for providence, guidance, and grace in seeing me through this study; I give HIM all the glory.

ACKNOWLEDGEMENT

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

I would also like to specially thank the head of department, Dr. Rosemary Usiobaifo, and other lecturers in the Department of Computer Science who I have been fortunate to cross paths with and who have impacted me immensely these past few years: Prof. (Mrs.) S. Konyeha, Prof. G. O. Ekuobase, Prof. K. C. Ukaoha, Prof. A. A. Imianvan, Prof. (Mrs.) F. Egbokhae, Prof. (Mrs.) V. V. N. Akwukwuma, Prof. F. I. Amadin, Prof. (Mrs.) V. I. Osubor, Dr. (Mrs.) Aziken, Dr. F. O. Chete, Dr. (Mrs.) R. O. Osaseri, Dr. F. O. Oliha, Dr. J. C. Obi, Mr. P. E. B. Imiefoh, Mr. I. E. Obasohan, Mr. K. O. Otokiti, Mr. I. E. Obayagbonna, Mrs. R. I. Izevbizua, Mr. E. C. Ighodan, Miss L. O. Usiosfe, Mr. J. Okhuoya, Prof. F. A. U. Imouokhome, Mrs. J. I. Adun, Dr. E. Nweli and Mr. D. Idehen.

I would also like to thank my family and friends for their support, words of encouragement, and consistent guidance throughout this project.

TABLE OF CONTENTS

ABSTRACT

This project aims to identify current and emerging phishing techniques and evaluate the level of awareness and preparedness among internet users, with the goal of proposing adaptive prevention measures.

The methodology involved reviewing advanced global phishing tactics (including deepfake video phishing and QR code phishing) and conducting a primary survey among Nigerian youths.

The study found that while exposure to phishing threats is high, the practical ability of users to correctly identify and prevent attacks is low, leaving them susceptible to scams like investment fraud and social media phishing. The project concludes that phishing is fundamentally a human-centric problem and proposes adaptive measures focused on integrating continuous education, practical simulation drills, and technological safeguards like 2FA to strengthen user vigilance.

CHAPTER ONE

Introduction

1.1 Background to the Study

In the ever-evolving landscape of cybersecurity threats, phishing techniques have become increasingly sophisticated, deceptive, and adaptive. These techniques form the operational backbone of phishing attacks, enabling cybercriminals to bypass both technological safeguards and human intuition. A core aspect of these techniques is the manipulation of human behavior through social engineering, often disguised within messages or interfaces that mimic legitimate platforms (*Arachchilage et al., 2021*). Phishing techniques have diversified significantly beyond traditional email-based scams. Modern attacks leverage a variety of channels and methods, including spear phishing, which customizes attacks based on specific targets; whaling, which focuses on high-level executives; and clone phishing, which duplicates legitimate communications to establish credibility (*Jayatilaka et al., 2024*). These are often supported by link manipulation, domain spoofing, and malicious attachments, which trick users into engaging with fake content. More recently, emerging methods such as quishing, the use of QR codes in phishing campaigns, have begun to exploit mobile device limitations, while smishing utilizes SMS messages to launch similar deceptions (*Weinz et al., 2025*). Attackers have also begun incorporating AI-generated content, making phishing emails more grammatically correct, contextually relevant, and personalized (*Rahartomo et al., 2025*). In some cases, attackers embed fake login pages that look indistinguishable from real sites, utilizing HTTPS certificates and visual elements cloned from legitimate sources. Techniques are also deployed in multi-stage attacks, where an initial contact (such as a survey or promotional offer) leads the user through a funnel of deception until credentials or financial information are obtained (*Sabo et al., 2023*). These evolving tactics often succeed by triggering emotions like urgency, curiosity, or fear, psychological levers that override rational judgment and encourage users to act impulsively. Despite the deployment of browser warnings, spam filters, and authentication protocols, the ingenuity of phishing techniques continues to outpace defense mechanisms. The growing complexity and realism of these methods make them difficult to detect, even for trained users, highlighting the urgent need to systematically analyze phishing techniques in depth. This study seeks to examine these methods as the central focus, identifying how they function, evolve, and exploit cognitive and contextual user vulnerabilities, with the ultimate aim of informing better prevention strategies and user education.

1.2 Statement of the Problem

In the age of ubiquitous internet access and digital dependence, phishing attacks continue to grow in scale and sophistication, despite the proliferation of advanced cybersecurity tools. Traditional technical defenses such as firewalls, spam filters, and antivirus software are no longer sufficient to stop phishing campaigns that cleverly disguise malicious intent behind a veneer of legitimacy. One of the primary challenges lies in the diverse and adaptive nature of phishing techniques. Attackers now utilize deep personalization through data breaches and open-source intelligence, exploit emotions such as fear or urgency, and leverage mobile platforms and QR codes in emerging formats like smishing and quishing. These methods evade conventional detection systems, making user education and behavioral preparedness more critical than ever. Furthermore, many internet users lack the cybersecurity awareness or digital literacy required to identify subtle phishing indicators such as mismatched URLs, spoofed domains, or unusual requests. This is particularly true across certain demographics, such as elderly users or low-experience digital users, who are disproportionately affected by these scams. Although public awareness campaigns exist, their reach and impact remain inconsistent. There is a lack of research evaluating how effective current strategies are in deterring specific types of phishing attacks. Without a deeper understanding of the techniques used and prevention strategies adopted by different user groups, cybersecurity interventions will remain inadequate and reactionary.

1.3 Aim and Objectives of the Study

Aim: This study aims to investigate the techniques used in phishing attacks and assess the effectiveness of existing prevention strategies among internet users, with the goal of proposing improved, user-centric cybersecurity measures.

Objectives:

1. To identify the common phishing techniques used to deceive internet users.
2. To evaluate the level of awareness and preparedness of different user groups against the identified phishing attacks.
3. To propose adaptive measures for improving phishing awareness and prevention efforts.

1.4 Research Questions

To guide the investigation of phishing cybersecurity attacks, the study will seek to answer the following key research questions:

1. What are the most common techniques and methods used by cybercriminals to carry out phishing attacks on internet users?

2. How aware are internet users of phishing threats, and what factors influence their level of awareness and susceptibility?
3. What are the major impacts of phishing attacks on individuals and organizations, including financial, psychological, and reputational consequences?
4. What types of prevention strategies and cybersecurity practices do internet users currently adopt to protect themselves from phishing attacks?
5. How effective are existing public awareness campaigns, cybersecurity education programs, and digital tools in helping users identify and avoid phishing attempts?
6. What role does digital literacy play in the ability of users to recognize and respond appropriately to phishing attempts?
7. To what extent do age, education level, occupation, and internet usage habits affect the likelihood of falling victim to phishing attacks?
8. How do different phishing attack vectors (e.g., email, SMS, social media, fake websites) vary in their success rates and user response behaviors?
9. What challenges do users face when attempting to verify the authenticity of online communications or websites?
10. What recommendations can be made to strengthen user preparedness, institutional defenses, and national cybersecurity policy in combating phishing attacks?

1.5 Research Hypotheses

This study is based on the premise that certain factors significantly influence internet users' exposure to phishing attacks, as well as the effectiveness of the strategies they adopt to protect themselves. One of the key hypotheses of this research is that internet users with a higher level of digital literacy and cybersecurity awareness are better equipped to recognize and avoid phishing attempts. Users who understand basic security principles, such as how to spot suspicious emails, verify URLs, and use secure authentication methods, are expected to demonstrate lower vulnerability compared to those with limited knowledge (*Arachchilage et al., 2021; Hafner et al., 2023*). Another hypothesis guiding the study is that the implementation of proactive cybersecurity practices, such as the use of two-factor authentication, spam filters, strong passwords, and updated antivirus software, substantially reduces the risk of falling victim to phishing attacks. These protective measures serve as additional layers of defense and are believed to be most effective when users are both aware of and consistently apply them (*Patel et al., 2022; Rahartomo et al., 2025*). It is also hypothesized that phishing attacks have a significant negative impact on victims, not only in terms of financial loss but also in psychological and emotional distress, erosion of trust in digital systems, and potential long-term reputational harm. These impacts may differ across user groups but are likely to be severe in cases involving identity theft or unauthorized financial transactions (*Tinubu et al., 2023; Yoshida et al., 2022*). Furthermore, the study hypothesizes that demographic variables such as age, level of education, occupation, and frequency of internet use play a significant role in determining how susceptible a user is to phishing attacks. For example, younger or more digitally literate individuals may be better at identifying scams, while less experienced users may be more easily deceived (*Wannenburg et al., 2023; Nadeem et al., 2022*). Lastly, it is assumed

that organized public awareness campaigns and cybersecurity education programs have a measurable positive effect on user behavior and preparedness. Users exposed to consistent and well-structured awareness efforts are more likely to adopt preventive behaviors and report suspicious activity, thereby contributing to a more resilient online environment (*Jensen et al., 2022; Canham et al., 2021*).

1.6 Significance of the Study

Phishing remains one of the most pervasive and damaging cybersecurity threats in the digital age, affecting millions of individuals and organizations worldwide. This study holds significant importance as it seeks to explore and understand the techniques used in phishing attacks, the various impacts on internet users, and the effectiveness of existing prevention strategies. The findings of this research are expected to contribute meaningfully to both academic knowledge and practical cybersecurity practices. For internet users, this study will raise awareness about the deceptive tactics employed by cybercriminals and highlight the importance of adopting secure online behaviors. By identifying common patterns and attack methods, the study aims to empower users with the knowledge needed to recognize, avoid, and report phishing attempts, thereby reducing their vulnerability. For organizations and cybersecurity professionals, the research provides insights into how phishing affects users at different levels and the challenges they face in implementing protective measures. This can help in designing more effective training programs, user interfaces, and security systems that prioritize human-centered design and behavior-based risk prevention. The study is also significant for educators and policymakers, as it underscores the need for incorporating digital literacy and cybersecurity awareness into educational curricula and national ICT policies. By understanding which strategies are most effective, stakeholders can develop more targeted and impactful awareness campaigns and interventions. Additionally, for the academic and research community, this study adds to the body of literature on cybersecurity, particularly in the context of user behavior, digital risk, and emerging threat landscapes. It provides a foundation for future research that could explore phishing across different demographics, industries, or technological environments. Overall, the study is timely and relevant in addressing the growing need for informed and proactive approaches to phishing prevention, helping to build a safer and more secure digital ecosystem for all users.

1.7 Scope of the Study

This study is centered on understanding the techniques used in phishing attacks and evaluating the prevention strategies adopted by internet users to combat such threats. It aims to investigate how phishing attacks are conducted, the deceptive methods used by cybercriminals, and how users perceive and respond to these threats. The research primarily focuses on two main aspects of phishing: the techniques employed by attackers and the preventive measures

currently in place among users across various demographics. The study will explore a range of phishing techniques, including but not limited to email phishing, spear phishing, smishing (SMS phishing), vishing (voice phishing), and clone phishing. These categories will be analyzed in terms of how they are designed, delivered, and executed, as well as the psychological manipulation strategies involved (e.g., urgency, authority, and fear-based messaging). The research will also consider both traditional and emerging phishing tactics, particularly as they relate to increasing internet usage and evolving digital communication platforms such as social media, messaging apps, and mobile devices. On the preventive side, the study will examine the awareness levels of internet users, their ability to identify phishing attempts, and the strategies they use to avoid falling victim to attacks. This includes both technical solutions (e.g., antivirus software, two-factor authentication, spam filters) and behavioral approaches (e.g., verifying URLs, avoiding suspicious links, cybersecurity training). The scope is limited to general internet users, including students, professionals, and everyday individuals who engage with the internet for communication, financial transactions, education, or entertainment. While organizational cybersecurity protocols are acknowledged, the primary focus remains on individual users' awareness and behavior. Geographically, the study may be confined to a specific region or country (e.g., Nigeria), depending on the availability of participants and data. Findings may not be universally generalizable but are expected to provide valuable insights into common phishing threats and user defenses within the chosen context.

CHAPTER TWO

Literature Review

This literature review examines a selection of key scholarly and practical contributions to the field of phishing awareness and prevention, with a specific focus on the techniques employed by various authors to study, measure, and enhance human resilience against phishing attacks. Rather than providing a broad survey of all available works, this chapter adopts an in-depth, analytical approach, scrutinizing each selected study for its methodological design, strengths, limitations, and potential for adaptation in contemporary contexts. By dissecting the techniques used across a range of research projects, spanning large-scale empirical studies, game-based learning interventions, immersive roleplay scenarios, multi-modal awareness campaigns, and real-world phishing simulations, this review seeks to understand not only what each study found, but how it arrived at those findings. Such a focus on methodology allows for critical evaluation of the practicality, scalability, and relevance of each approach in today's rapidly evolving threat landscape.

2.1 An In-Depth Analysis of the "Think-Aloud" Method in Jayatilaka et al.'s 2021 Study on Phishing Susceptibility: Effectiveness, Limitations, and Modern Applicability

Unlike many cybersecurity challenges that can be countered with software patches or system upgrades, phishing fundamentally targets the human element, relying on manipulation, deception, and social engineering tactics. In this light, behavioral studies that explore how individuals respond to suspicious messages are indispensable for designing more effective prevention and awareness strategies. Among such contributions, the work of Jayatilaka, Arachchilage, and Babar in their 2021 paper, *Falling for Phishing: An Empirical Investigation into People's Email Response Behaviours*, stands out as an insightful examination into the cognitive and emotional processes that lead users to fall victim to phishing attempts. The study's central methodological innovation was the application of the "think-aloud" approach to phishing research, involving nineteen participants who were asked to process emails while verbalizing their thought processes in real-time. This method allowed researchers to go beyond superficial metrics such as click rates and instead explore the underlying reasoning, heuristics, and affective triggers that drive email-handling decisions. Such a qualitative approach was particularly significant in a field often dominated by quantitative, large-scale phishing simulations that, while valuable, tend to reduce user behavior to binary outcomes ("clicked" or "did not click") without revealing the nuanced psychological journey leading to those actions. The think-aloud

technique, as implemented in this study, required participants to articulate every thought, impression, and decision as they engaged with email content. By narrating their reasoning, they revealed factors such as perceived legitimacy cues, the influence of urgent or alarming language, the role of familiarity with the sender, and the perceived relevance of the message's subject matter to their own lives. This level of introspection generated a rich dataset of verbal protocols, enabling the identification of eleven key influencing factors that affected phishing susceptibility. Among these factors were trust in known brands, the presence or absence of grammar errors, visual presentation, alignment with the recipient's personal or professional context, and emotional triggers such as fear or opportunity. From an effectiveness standpoint, the method proved highly capable of uncovering subtle, often subconscious, decision-making influences. Unlike post-hoc surveys or retrospective interviews, which rely on participants' memory and self-awareness, the think-aloud approach captures cognitive processes as they unfold in real time, thereby reducing the distortion that often arises from memory bias or rationalization after the fact. In the domain of phishing research, where the difference between clicking a link and ignoring it can be decided in a matter of seconds, having access to an unfiltered stream of cognitive data is invaluable. Moreover, the small-group, observational setting allowed for close monitoring by the researchers, ensuring that even fleeting remarks or hesitations could be noted and analyzed for patterns. However, despite these strengths, the method is not without its limitations. The most immediate constraint was the small sample size (only nineteen participants), which inevitably raises concerns about generalizability. While the insights derived from such a cohort are deep, they cannot be assumed to represent the full diversity of internet users, especially given variations in digital literacy, cultural background, and personal exposure to phishing. Furthermore, the laboratory environment in which the study took place may have inadvertently influenced participant behavior. Knowing that one is part of a study often leads to the so-called "Hawthorne effect," where individuals alter their behavior simply because they are being observed. In a real-world phishing encounter, absent the artificiality of a controlled setting, participants might behave more impulsively or less cautiously. Another challenge lies in the cognitive load imposed by the think-aloud requirement. Verbalizing thought processes in real-time is not a natural activity for most individuals, and the act of having to articulate one's reasoning might itself slow down decision-making or prompt more deliberate reflection than would occur in an everyday context. This could mean that the study's data, while rich, may reflect a more cautious and analytical approach to email assessment than would be typical in a user's routine inbox interactions. In other words, participants might have been more skeptical or meticulous simply because they were consciously engaged in narrating their decision-making process. When assessing whether the think-aloud method should be considered exemplary and widely adopted in modern phishing research, it is important to situate the discussion in the context of evolving phishing tactics. In 2021, phishing emails were already becoming sophisticated, but in the years since, the landscape has changed significantly. Advances in artificial intelligence have enabled attackers to craft highly convincing, grammatically flawless messages, even generating personalized content tailored to individual targets. Phishing has also expanded beyond email to encompass smishing (SMS phishing), vishing (voice phishing), and social media-based lures. The think-aloud method's strength lies in its ability to expose the reasoning process behind a user's decision to trust or distrust a message, and this is just as relevant, if not more so, in the age of AI-driven cybercrime. Despite

the methodological and logistical challenges, the core premise of Jayatilaka et al.'s study, that deep insight into user psychology can be gained by listening to their real-time reasoning, remains compelling. While large-scale click-rate analyses are valuable for measuring the prevalence of phishing susceptibility, they cannot explain why people fall for scams. Without understanding the "why," defenses remain reactive and superficial. The think-aloud method, properly adapted and scaled, has the potential to bridge this gap, providing the kind of human-centered intelligence that technical countermeasures alone cannot deliver. In conclusion, the think-aloud method as used by Jayatilaka, Arachchilage, and Babar in their 2021 investigation was a bold and insightful choice, yielding rich qualitative data that illuminated the complex interplay of cognitive, emotional, and contextual factors influencing phishing susceptibility. While its small sample size and artificial setting limit its generalizability, these weaknesses are not inherent to the method itself but rather to the constraints of the particular study. With strategic enhancements, including larger, more diverse participant pools, integration with real-world simulations, adoption of complementary data collection technologies, and expansion to multi-channel phishing scenarios, the think-aloud approach could become an exemplary tool in modern phishing research. In an era where cybercriminals are leveraging increasingly sophisticated psychological and technological strategies, the ability to peer directly into the decision-making process of potential victims is not just academically valuable; it is a practical necessity for the development of effective defenses.

2.2 An Analytical Review of Lain et al.'s 2021 Study on Phishing in Organizations: Long-Term Simulation Insights, Strengths, Limitations, and Modern Implications

Phishing remains one of the most effective cyberattack vectors against organizations, largely because it exploits human behavior rather than technical flaws. Even in environments equipped with state-of-the-art security software, the human element often represents the weakest link in the security chain. For this reason, organizations worldwide have invested heavily in phishing simulations, awareness campaigns, and employee training programs. Yet a critical question remains: How effective are these efforts in the long term, and do they produce lasting behavioral change? In their 2021 study, *Phishing in Organizations: Findings from a Large-Scale and Long-Term Study*, Lain, Kostiainen, and Capkun offer valuable empirical evidence addressing these questions. What makes this study stand out is its scale and duration. Unlike many phishing research projects that run for a few weeks or focus on small, non-enterprise populations, this investigation spanned 15 months and involved approximately 14,000 employees within a single organization. The methodology centered on real-world phishing simulations, embedded into the organization's regular email traffic, and aimed at assessing employee resilience over time. The large participant base and extended duration enabled the authors to observe not just initial responses but also changes, if any, in phishing susceptibility as employees were exposed to repeated simulated attacks and embedded awareness measures. The core technique used in the study was the enterprise-wide phishing simulation program. Employees were sent a series of crafted phishing emails designed to mimic real-world malicious

messages, complete with varied subject lines, senders, and content themes. The emails were timed at irregular intervals to reduce predictability and were blended into normal workflow communications to simulate realistic attack conditions. The study's aim was to measure how often employees clicked on malicious links or engaged with phishing content and how these rates evolved with time and exposure to embedded awareness reminders. From an operational standpoint, the scale of the study is impressive. Large-scale enterprise simulations provide a rare opportunity to observe authentic user behavior in the natural context of work. Unlike controlled lab settings, where participants are consciously aware of being studied, simulations embedded into the flow of daily work can capture more genuine reactions. In this regard, the method has a significant advantage in ecological validity. The participants, unaware of the exact nature or timing of the simulations, responded as they would to any other incoming email, providing researchers with data that is arguably closer to real-world conditions than most experimental setups. However, the study's findings present a sobering reality: embedded training alone was not sufficient to significantly improve resilience. Despite repeated exposure to simulations and corresponding awareness materials, phishing click rates did not decline substantially over the 15-month period. This suggests that awareness training, at least in the form deployed during the study, may not be enough to effect durable behavioral change in organizational contexts. The authors interpret this as evidence that while awareness campaigns are a valuable component of a defense strategy, they must be complemented by strong technical controls, such as email filtering, link scanning, and multi-factor authentication, to effectively mitigate phishing risks. The strength of this technique lies in its ability to gather large quantities of behavioral data over an extended time frame. This allows for nuanced trend analysis, such as determining whether there is a learning curve among employees or whether susceptibility fluctuates depending on time of year, workload, or other contextual factors. Furthermore, the diversity of roles, departments, and responsibilities within a large organization ensures that the data captures a variety of user behaviors and exposures to phishing risk. Nevertheless, the method also carries certain limitations. The most obvious is the single-organization scope. While 14,000 participants is an impressive sample size, the findings are necessarily shaped by the organizational culture, security policies, and work environment of that specific company. A highly regulated financial institution, for example, might have a workforce that responds differently to phishing than a tech startup or a manufacturing firm. This means that while the study offers valuable internal insights, its generalizability to other organizational contexts is somewhat limited. Another potential limitation is the nature of the phishing emails used in the simulation. If the crafted messages were too obvious or too generic, employees might have been more likely to detect them than they would a real-world spear-phishing attempt crafted with detailed personal or departmental information. Conversely, if the simulated emails were too sophisticated, the resulting click rates might have painted an unduly pessimistic picture of employee resilience. Striking the right balance in simulation realism is a persistent challenge in phishing research, as overly simplistic scenarios risk underestimating susceptibility, while overly complex ones risk demoralizing staff or creating mistrust in internal communications. Moreover, the study highlights a critical behavioral insight: awareness fatigue. Employees exposed to repeated training messages or phishing tests may begin to tune them out, reducing the effectiveness of these interventions over time. This phenomenon mirrors patterns seen in other domains of workplace safety training, where the

novelty of the intervention wears off, and compliance becomes perfunctory rather than thoughtful. In the context of phishing, this may mean that while employees are aware of the need to be cautious, they fail to apply that caution consistently in practice. From a modern perspective, the study's implications are highly relevant. As phishing evolves to include AI-generated content, deepfake videos, and multi-channel campaigns, the challenge for organizations is no longer just to train employees to spot grammatical errors or suspicious URLs. Attackers can now produce flawless, personalized messages that mimic trusted contacts with uncanny accuracy. In this context, the Lain et al. study reinforces the idea that relying solely on awareness training is insufficient. Modern defenses must adopt a layered security model, where human vigilance is supported by advanced technical barriers capable of detecting and neutralizing threats before they reach end-users. Furthermore, the study offers a cautionary note against complacency in training program design. A 15-month program without measurable improvement in resilience suggests that training approaches must be continuously evaluated and adapted. Static programs that repeat the same content over long periods are unlikely to keep pace with the sophistication and variability of modern phishing campaigns. In conclusion, the large-scale, long-term simulation conducted by Lain, Kostiainen, and Capkun in 2021 provides both a methodological benchmark and a strategic warning for modern cybersecurity practice. The enterprise-scale deployment, with its authentic integration into daily workflows, offers a model of ecological validity that should be emulated in future research. However, the study's findings, that embedded awareness training alone is insufficient to significantly improve organizational resilience, highlight the urgent need for multifaceted strategies that combine ongoing, adaptive awareness efforts with robust technical safeguards. For researchers, the lesson is clear: to truly understand and counteract phishing susceptibility in the workplace, studies must be both large in scale and diverse in scope, while remaining agile enough to adapt to the rapidly shifting tactics of cyber adversaries.

2.3 An Evaluation of PHISHGEM: Mobile Game-Based Learning for Phishing Awareness: Strengths, Weaknesses, and Modern Implementation Potential

Phishing has evolved from rudimentary, mass-mailed scams to sophisticated, targeted attacks capable of deceiving even well-trained individuals. Traditional training approaches, such as static e-learning modules, annual workshops, and generic awareness campaigns, have been criticized for their inability to engage users effectively or sustain learning over time. In response, cybersecurity educators and researchers have increasingly explored gamification as a method to enhance engagement, motivation, and knowledge retention in security training. It is within this context that PHISHGEM: A Mobile Game-Based Learning for Phishing Awareness, developed by Tinubu, Falana, and Oluwumi in 2023, stands out as a promising and innovative approach to phishing education. PHISHGEM is designed as an interactive mobile game that aims to teach players about common phishing tactics in a playful yet educational environment. The game incorporates scenarios modeled after real-world phishing attempts, including deceptive links, spoofed domains, urgent call-to-action messages, and brand impersonation techniques. Users

navigate through these scenarios, making decisions on whether to trust or report suspicious content, and receive immediate feedback based on their choices. The primary objective is not merely to inform players of phishing concepts but to train recognition skills through repeated practice and reinforcement, all within the accessible, engaging framework of a mobile gaming app. The methodology behind PHISHGEM's evaluation involved field testing with 100 participants, who played the game and were then assessed on their phishing awareness levels. The results were striking: the game achieved 98% awareness rates among participants, with high usability scores and positive engagement feedback. This demonstrates the method's capacity to transform a traditionally tedious topic into an enjoyable, repeatable, and effective learning experience. Participants not only absorbed knowledge but also developed a sense of confidence in identifying and responding to phishing attempts. The technique used (mobile game-based learning) has several intrinsic advantages for phishing awareness campaigns. First, it leverages interactivity, which has been proven to significantly improve learning retention compared to passive instruction. In a gaming environment, users are active participants, making choices and receiving instant consequences for those choices, rather than passively consuming information. Second, the mobile platform ensures accessibility and convenience. Since most individuals carry smartphones and have frequent idle moments, a mobile game allows learning to happen anytime and anywhere, seamlessly fitting into daily routines. Third, gamification taps into intrinsic motivators such as curiosity, achievement, and competition. By incorporating levels, scores, badges, or leaderboards, the learning process becomes self-reinforcing, encouraging players to replay and deepen their understanding. However, despite these strengths, PHISHGEM's methodology is not without limitations. The participant pool of 100 users, while reasonable for a pilot evaluation, is relatively small and may not reflect the diversity of the global internet-using population. Furthermore, the study does not clearly specify the demographic diversity of its participants, an important factor given that age, educational background, cultural context, and digital literacy can influence both gameplay engagement and susceptibility to phishing. Another limitation is the lack of longitudinal measurement. While participants showed high awareness immediately after playing the game, it remains unclear how much of this knowledge and skill persisted weeks or months later. Without follow-up studies, we cannot determine whether PHISHGEM's impact is lasting or if it requires periodic re-engagement to maintain efficacy. In terms of content realism, game-based phishing simulations face a unique challenge: balancing authenticity with playability. Real phishing emails may involve subtle cues, such as minute differences in domain names, nuanced language inconsistencies, or slightly altered branding, that are harder to replicate in a visually engaging mobile game format. If the in-game phishing scenarios are oversimplified, they risk failing to prepare players for the full complexity of real-world attacks. On the other hand, overly realistic scenarios may make the game too difficult or discouraging, reducing engagement. Striking the right balance is essential for maximizing both learning outcomes and user enjoyment. From a modern implementation perspective, PHISHGEM has significant potential as part of a multi-layered phishing defense strategy. While no training method can guarantee zero clicks, embedding mobile game-based learning into a broader security awareness program could yield measurable improvements in employee vigilance. This is especially true in hybrid or remote work environments, where employees are often outside the immediate supervision of IT departments and may rely more heavily on personal judgment to assess suspicious messages. Furthermore, mobile games can

transcend organizational boundaries, reaching populations that might not otherwise receive formal phishing awareness training, such as freelancers, retirees, or individuals in developing regions with limited access to traditional cybersecurity education. The appeal of PHISHGEM also lies in its scalability. Once developed, a mobile game can be distributed at minimal cost per user, allowing mass deployment without the logistical constraints of classroom training or in-person workshops. Updates can be delivered remotely, ensuring that content remains relevant without requiring significant additional infrastructure. Additionally, gamified training produces measurable engagement metrics, such as level completion rates, time spent in-game, and accuracy in identifying phishing scenarios, that can be analyzed to assess learning progress and refine content. Critically, however, PHISHGEM should be seen not as a standalone solution but as a complement to other measures. Phishing is a constantly evolving threat, and while awareness training is essential, it must be supported by technical safeguards such as advanced email filtering, sandboxing of suspicious attachments, and multifactor authentication. The game can equip users with knowledge and recognition skills, but organizations must still assume that some attacks will bypass human detection and rely on layered defenses to catch them. In conclusion, PHISHGEM: A Mobile Game-Based Learning for Phishing Awareness represents an innovative and promising direction in cybersecurity education. By combining the accessibility of mobile platforms with the motivational power of gamification, it addresses key weaknesses in traditional awareness training and demonstrates the potential to engage users in a meaningful, enjoyable learning process. While the initial evaluation results are encouraging, boasting 98% awareness among participants, the methodology can be strengthened through larger and more diverse participant samples, adaptive content difficulty, real-world scenario integration, and ongoing engagement mechanisms. In the modern threat landscape, where phishing attacks are increasingly sophisticated and relentless, PHISHGEM offers a creative, scalable, and potentially transformative tool for building resilience among both organizational employees and the general public.

2.4 An In-Depth Review of Rahartomo et al.'s 2025 "Phishing Awareness via Game-Based Learning": Innovative Techniques, Measured Impact, and Recommendations for Modern Application

Phishing attacks have continued to evolve at an alarming pace, with attackers leveraging increasingly sophisticated deception tactics to bypass both technical and human defenses. In this climate, awareness training has remained a critical pillar of cybersecurity strategy. However, as research has repeatedly shown, traditional lecture-based or text-heavy training programs often fail to hold learners' attention or foster lasting behavioral change. In recent years, the use of game-based learning has emerged as an innovative alternative, blending education with interactive, immersive engagement to better equip individuals against phishing threats. It is within this context that the work of Rahartomo, Ghaleb, and Ghafari in their 2025 study, *Phishing Awareness via Game-Based Learning*, contributes valuable insight into the potential of gamified approaches to cybersecurity awareness. The study set out with the explicit goal of enhancing

user awareness of phishing through a serious game, a game designed not for pure entertainment but for targeted educational purposes. The game simulated various phishing scenarios, including clone phishing, SMS phishing (smishing), and spear phishing. Each scenario presented players with realistic-looking messages, requests, and cues that they had to evaluate and respond to appropriately. The gameplay mechanics required participants to make decisions (such as clicking a link, reporting the message, or ignoring it) while receiving feedback on the correctness of their actions. By doing so, the game aimed to create a learning loop in which players could quickly understand their mistakes and internalize correct detection strategies.

The technique used (immersive scenario-based game learning) allowed participants to experience phishing encounters in a safe, controlled environment. Importantly, this game was not limited to email-based attacks. By incorporating SMS and spear phishing, the study acknowledged the modern reality that phishing is no longer confined to inboxes. Attackers now exploit multiple communication channels, often combining them in multi-stage campaigns designed to exploit trust and urgency across different platforms. The inclusion of these varied scenarios thus mirrors the complexity of the contemporary threat landscape. The evaluation involved 28 participants, who engaged in the game before and after an awareness measurement process. Results showed a 24% increase in awareness and a 30% increase in confidence when identifying phishing attempts after gameplay. These figures, while based on a relatively small sample, suggest that game-based learning can deliver measurable improvements in both knowledge and self-efficacy, the latter being particularly important, as individuals who are confident in their ability to detect phishing are more likely to act decisively when faced with a suspicious message. The strengths of this approach are clear. First, the variety of attack vectors simulated in the game makes the training relevant to modern conditions. Whereas some awareness tools focus narrowly on email phishing, Rahartomo et al.'s design recognizes that phishing manifests in text messages, instant messaging apps, and even voice communications. By preparing users for a broader set of threats, the training increases their adaptability in real-world situations. Second, the interactivity and feedback loop inherent in gaming significantly enhance knowledge retention compared to passive learning methods. Immediate feedback ensures that mistakes are corrected in the moment, while repetition across different scenarios reinforces correct behavior. This stands in contrast to annual corporate training sessions, where information may be forgotten long before it is needed. Third, the confidence boost observed in participants is a crucial, if often underappreciated, outcome. A well-informed but hesitant employee can still fall victim to phishing if they doubt their ability to correctly assess a message. By improving self-efficacy, the game not only equips users with knowledge but also empowers them to act on that knowledge decisively. That said, the methodology does have notable limitations. The sample size, just 28 participants, is too small to support broad generalization. The demographics of the group are not detailed, making it unclear whether the participants represented a diverse range of ages, professions, and technical skill levels. Such factors are important, as digital literacy and prior exposure to phishing threats can greatly influence both learning outcomes and gameplay engagement. Another limitation is the short-term nature of the study. While post-game awareness and confidence gains were impressive, there is no evidence as to whether these improvements persisted weeks or months

later. Without longitudinal tracking, it is impossible to determine whether the observed gains reflect true learning or simply a temporary boost from recent exposure. Additionally, while the game's inclusion of multiple phishing types is commendable, the realism of the scenarios is not described in detail. Effective phishing simulations must strike a delicate balance between realism and user engagement. If the scenarios are overly simplified, they risk leaving players ill-prepared for the subtlety and sophistication of modern attacks, particularly those crafted using AI to mimic writing styles, brand identities, or personal contacts. Conversely, if the scenarios are too complex or frustrating, players may disengage, undermining the training's effectiveness. From a modern applicability standpoint, Rahartomo et al.'s approach is highly relevant. In 2025, phishing campaigns increasingly use multi-channel and AI-driven tactics, meaning that awareness training must equip users to detect and respond to attacks across diverse mediums. The game-based approach, particularly one that covers email, SMS, and spear phishing, is well-suited to preparing users for this expanded threat surface. Moreover, this method holds promise not only in corporate environments but also in public education initiatives. With phishing targeting individuals of all ages and backgrounds, from students to retirees, mobile or web-based game training could be deployed on a large scale through schools, community centers, and online awareness campaigns. The flexibility of the game format means that it can be distributed widely and updated easily, maximizing reach and relevance. In conclusion, Rahartomo, Ghaleb, and Ghafari's *Phishing Awareness via Game-Based Learning* offers an innovative and engaging alternative to traditional phishing awareness training. Its strengths lie in its scenario diversity, interactive feedback, and measurable improvements in both awareness and confidence. However, the small sample size and lack of longitudinal measurement limit the strength of its conclusions. By scaling up participation, incorporating adaptive difficulty, integrating real-time phishing intelligence, and building in periodic refreshers, the methodology could be refined into a powerful, widely deployable tool for combating phishing in the modern era. In a threat landscape where attackers continually adapt, such dynamic, immersive training methods may well be essential for staying one step ahead.

2.5 A Comprehensive Analysis of Jensen et al.'s 2022 Study on Gamification for Phishing Reporting: Technique, Effectiveness, and Modern Applications

In the battle against phishing, organizations often focus their efforts on preventing employees from clicking on malicious links or engaging with fraudulent requests. While this is an essential aspect of cybersecurity training, it overlooks a critical component of an effective defense strategy: reporting. When a phishing email reaches an employee's inbox, and that employee recognizes it as suspicious, the ideal next step is not merely to ignore or delete it but to report it to the appropriate security team. Prompt reporting allows for rapid incident response, enabling organizations to block similar emails, warn other employees, and investigate potential breaches. However, in practice, phishing reporting rates remain frustratingly low in many organizations. Employees may recognize a threat but fail to report it due to lack of confidence, uncertainty about the reporting process, or the perception that it is not worth the effort. This is where the

2022 study by Jensen, Wright, Durcikova, and Karumbaiah, *Improving Phishing Reporting Using Security Gamification*, makes a significant contribution. The research explored how gamification, the integration of game design elements into non-game contexts, can be used to incentivize and improve phishing reporting behavior. The technique employed in the study involved embedding gamified elements into the phishing reporting process within a simulated office environment. The researchers tested mechanisms such as incentives, leaderboards, and feedback systems to encourage users to report suspected phishing emails more consistently and quickly. These elements were integrated into realistic simulations, ensuring that participants' behavior reflected how they might respond in a real-world work setting. The use of incentives could take multiple forms, ranging from points awarded for correct phishing reports to small tangible rewards such as gift cards or recognition in company newsletters. Leaderboards displayed top performers, creating a sense of friendly competition among employees. Feedback systems provided immediate confirmation of whether a report was accurate, helping users reinforce correct identification skills. The results were encouraging: both incentives and feedback were found to increase reporting rates. In particular, the combination of competition and positive reinforcement appeared to create a self-sustaining loop, where employees became more proactive in identifying and reporting threats. Importantly, the study showed that reporting behavior could be influenced not just by formal policies or training sessions, but by making the act of reporting itself engaging and rewarding. This approach offers several strengths. First, gamification addresses a behavioral gap that traditional training often overlooks. Employees may know how to identify phishing but still fail to act on that knowledge; gamification bridges this gap by making the reporting process itself more attractive. Second, by providing instant feedback, gamification allows for real-time learning. If an employee mistakenly reports a legitimate email as phishing (a "false positive"), they can immediately learn why it was safe, reducing over-reporting in the future. Third, gamification taps into both intrinsic and extrinsic motivation. While some employees may be driven by the personal satisfaction of topping a leaderboard, others may be motivated by tangible rewards or recognition. By appealing to multiple motivational drivers, gamification has the potential to engage a wider range of personalities and work styles. However, the methodology is not without limitations. One potential drawback is the risk of false positives; employees might over-report safe emails simply to gain points or climb the leaderboard. This could create noise for security teams, who must sift through excessive reports to find genuine threats. To mitigate this, the point system must be carefully designed to reward accuracy as much as frequency, ensuring that quantity does not overshadow quality. Another limitation is sustainability. Gamification can produce strong short-term gains in engagement, but there is a risk that interest will wane over time if rewards become repetitive or predictable. In long-term implementations, the novelty of competition and incentives may fade, leading to a decline in reporting rates unless new elements are periodically introduced to refresh the experience. Additionally, gamification strategies must be sensitive to organizational culture. In competitive work environments, leaderboards can motivate employees, but in more collaborative or non-hierarchical cultures, they may foster resentment or anxiety. Careful design is needed to ensure that gamified elements align with the organization's values and do not inadvertently create unhealthy competition. In the context of modern phishing threats, gamification is particularly relevant. Phishing campaigns have grown increasingly complex, often blending social engineering with AI-generated content and deepfake impersonations. The

speed at which threats must be reported has also increased; in some cases, a single malicious email can be sent to thousands of employees within minutes. Encouraging rapid, accurate reporting through gamification not only improves the organization's security posture but also transforms employees into active participants in defense rather than passive recipients of security instructions. Moreover, this approach could be integrated into broader security awareness ecosystems. For example, points earned from phishing reporting could be combined with points from other security-related activities, such as completing training modules, using strong passwords, or enabling multi-factor authentication. This would encourage holistic engagement with cybersecurity practices, not just phishing defense. In conclusion, Jensen, Wright, Durcikova, and Karumbaiah's *Improving Phishing Reporting Using Security Gamification* offers an innovative approach to bridging the gap between knowledge and action. By making the act of reporting phishing both engaging and rewarding, the technique addresses a persistent weakness in organizational defenses. While careful design is needed to prevent false positives, ensure sustainability, and align with organizational culture, the potential benefits are significant. In a time when cyber threats are both more sophisticated and more rapid in their execution, gamified reporting systems could play a pivotal role in transforming employees from passive observers into active defenders of organizational security.

2.6 An In-Depth Examination of Sabo et al.'s 2023 IMPAWSTER Program: Roleplay-Driven Phishing Awareness, Strengths, Limitations, and Modern Relevance

Phishing awareness training has long faced the challenge of keeping participants engaged while imparting skills that will be retained and applied in real-world scenarios. Many conventional approaches, such as lecture-based sessions or static e-learning courses, risk being perceived as dull, overly theoretical, or disconnected from the fast-paced, unpredictable nature of phishing attacks. In response to these shortcomings, IMPAWSTER, developed by Sabo, Black, and Sarno in 2023, introduced an innovative training method that combined simulated phishing exercises with interactive email roleplay. The central idea behind IMPAWSTER was to move beyond passive learning and instead immerse participants in a dynamic, narrative-driven environment. The program was framed around a spy-themed storyline, where trainees assumed roles as either attackers or defenders in simulated phishing scenarios. This framing not only added a layer of engagement and entertainment but also allowed participants to experience phishing from multiple perspectives, both as a target and as the orchestrator of a phishing campaign.

The technique integrated two core elements:

1. **Simulated phishing exercises:** Participants received realistic phishing emails designed to mimic real-world attack patterns, including common tactics such as spoofed addresses, urgency cues, and enticing offers.

2. **Email roleplay:** In guided sessions, participants composed and sent simulated phishing messages to others in the training group, attempting to craft convincing attacks. They then received feedback from trainers and peers on the effectiveness and detectability of their attempts.

This dual perspective (experiencing phishing as both victim and attacker) was central to the training's design philosophy. By crafting phishing messages themselves, participants gained insight into the psychology, social engineering principles, and technical details that underpin such attacks. This deeper understanding enhanced their ability to recognize similar tactics when encountered in real life. The study was conducted as a controlled user experiment, measuring participants' phishing awareness before and after training. Results indicated that roleplay significantly increased engagement levels and improved participants' ability to detect phishing cues. The novelty of the spy theme and the competitive element of crafting believable phishing emails appeared to enhance motivation and participation rates compared to traditional awareness sessions. Several strengths emerge from this approach. First, the immersive narrative provided by the spy theme leveraged storytelling as a learning tool. Narrative immersion is known to enhance retention because learners become emotionally invested in the scenario, making the lessons more memorable. Second, the attacker's perspective is a rare but valuable addition to phishing awareness training. Understanding how phishing campaigns are constructed and what makes them effective equips participants with a more nuanced mental model of threats, thereby improving detection skills. Third, the program's active learning format aligns with modern educational best practices, where learners are participants rather than passive recipients. By actively engaging in phishing detection and creation tasks, trainees practice critical thinking and pattern recognition in real time, skills that directly translate to their day-to-day interactions with digital communications. However, the methodology has limitations. One is the short-term evaluation period. The study measured improvements in awareness immediately after the training but did not track whether these gains persisted over time. This is a recurring challenge in cybersecurity awareness research: without longitudinal studies, it is difficult to determine the lasting impact of any training program. Another limitation concerns scalability. While roleplay is highly engaging, it is also resource-intensive. Facilitating interactive sessions where participants craft and exchange phishing emails requires skilled trainers, controlled environments, and coordination among participants. This makes it harder to deploy at scale in large organizations compared to automated, simulation-based campaigns. Additionally, the theme and format may not appeal to all audiences. While the spy motif might engage some learners, others might perceive it as gimmicky or distracting from the seriousness of the topic. Training programs must be adaptable to different organizational cultures and demographics, ensuring that the style of delivery does not alienate participants or undermine the perceived importance of the training. From a modern threat perspective, the IMPAWSTER approach remains highly relevant. Cybercriminals increasingly employ personalized, spear-phishing tactics that require vigilant, context-aware employees to detect. By training individuals to think like attackers, roleplay exercises cultivate a deeper understanding of these tactics, which is critical in combating sophisticated threats. Moreover, phishing campaigns today are often multi-channel (spanning email, SMS, and even social media), which means that teaching the underlying principles of deception (rather than simply memorizing common red flags) is crucial for cross-channel detection. In conclusion, IMPAWSTER represents an innovative fusion of

simulation and roleplay that addresses key weaknesses in conventional phishing awareness programs. By combining victim and attacker perspectives within an engaging narrative, the method promotes active learning, deeper understanding, and higher engagement. While its scalability and long-term retention remain challenges, these can be mitigated through modular design, digital delivery, and periodic refreshers. In an era of increasingly personalized and convincing phishing campaigns, the IMPAWSTER model stands out as a creative and impactful training method that has the potential to significantly strengthen human defenses against social engineering attacks.

2.7 A Detailed Examination of Hafner et al.'s 2023 TASEP Training Approach: Tabletop Role-Playing for Phishing and Social Engineering Awareness

One of the consistent challenges in cybersecurity training is finding methods that are both engaging and effective over the long term. Employees often regard security awareness programs as an obligation rather than an opportunity for professional development, leading to disengagement and low retention of critical knowledge. Hafner, Wutz, Pöhn, and Hommel's 2023 work, *TASEP: A Collaborative Social Engineering Tabletop Role-Playing Game*, offers a novel answer to this problem by applying the tabletop role-playing game (RPG) format, traditionally associated with entertainment, to the serious purpose of phishing and social engineering awareness. The name TASEP stands for Tabletop Awareness for Social Engineering Prevention. As the title suggests, the game's design focuses not only on phishing emails but also on broader social engineering tactics, recognizing that modern phishing attacks are often part of multi-stage campaigns that exploit various forms of human interaction. These can include phone calls (vishing), text messages (smishing), in-person impersonation, and hybrid attacks combining digital and physical elements. The technique involves groups of participants collaboratively playing through fictional but realistic scenarios in which they must identify, respond to, and mitigate social engineering attempts. Unlike passive awareness training, tabletop role-playing places participants directly into interactive storylines where they must make decisions collectively, debate potential courses of action, and face the consequences of their choices. During a typical session, players are given a scenario outline, for example, a sudden email from a supposed supplier claiming a payment issue, followed by a phone call from the "supplier" confirming the urgency of the request. The group must decide whether to act, escalate, verify the claim, or ignore it. The facilitator introduces twists and variables as the game progresses (such as fake but convincing invoices, suspicious USB drives, or conflicting information from internal sources), forcing players to reassess their assumptions. The collaborative element of TASEP is key. In real organizations, phishing and social engineering threats rarely affect just one person; they often involve communication between multiple team members. By having participants discuss and defend their decisions within the game, TASEP trains them to articulate their reasoning and challenge one another constructively, skills that translate well to real-world situations where quick, collective decisions are necessary. According to the authors, the game was primarily evaluated through student

participation in an academic setting. Students reported that the format was more engaging than traditional awareness lectures, and post-game assessments indicated improved understanding of social engineering tactics and phishing detection cues. The engagement factor was especially notable, many participants expressed enthusiasm about the training, a stark contrast to the reluctance often observed in standard corporate awareness sessions. The strengths of this method are several. First, immersive storytelling in tabletop role-playing helps embed lessons in memory by linking them to emotionally charged, narrative experiences. Rather than memorizing a checklist of red flags, players recall how they responded to specific in-game challenges, making the learning more intuitive and applicable. Second, the group decision-making component fosters a shared responsibility for security. This aligns well with the reality of organizational defense, where culture and collective vigilance matter just as much as individual skill. Employees who have practiced discussing and justifying security decisions are more likely to speak up in real situations, reducing the chance that a single point of failure will result in a breach. Third, the customizability of the tabletop format means that scenarios can be adapted for different audiences. For example, scenarios for finance teams might focus on invoice fraud and wire transfer scams, while IT staff might face simulated credential-harvesting attempts targeting admin accounts. Despite these strengths, TASEP also faces limitations. One is scalability; as with many interactive, facilitator-led methods, the tabletop format is inherently resource-intensive. Each session requires a trained facilitator, preparation of materials, and coordination among participants, which can be difficult to replicate across large, geographically dispersed organizations. Another limitation is that the study's evaluation was conducted in an academic context. While students can provide valuable feedback, they may not face the same time pressures, responsibilities, or real-world consequences as working professionals. The effectiveness of TASEP in high-stress corporate environments has yet to be fully validated. Additionally, while the game is engaging, there is a risk that participants might over-associate the scenarios with the game's fictional setting. If the in-game scenarios are too far removed from participants' actual work environments, the transfer of skills to real-world situations could be weakened. This is a common risk in gamified training; lessons must be clearly and explicitly linked to real-life application. From a modern perspective, TASEP's emphasis on collaboration and narrative immersion is highly relevant. In 2025, phishing attacks are increasingly complex, often using multi-channel approaches that require team-based detection and response. AI-generated phishing content, for instance, can be tailored to specific roles within a company, making it harder for individuals to rely solely on personal experience or instinct. Collaborative training like TASEP prepares employees to approach security threats as collective challenges rather than individual puzzles. In conclusion, Hafner et al.'s *TASEP: A Collaborative Social Engineering Tabletop Role-Playing Game* offers an engaging and highly interactive model for phishing and social engineering awareness. Its strengths in immersion, teamwork, and adaptability make it a compelling alternative to more traditional, lecture-based methods. While its scalability and workplace applicability need further exploration, TASEP stands out as an innovative approach that could significantly enhance security culture when implemented thoughtfully. By transforming training into a shared, story-driven experience, it not only teaches detection skills but also builds the collaborative mindset essential for defending against modern, multifaceted cyber threats.

CHAPTER THREE

The Evolving Landscape of Phishing Threats and Vulnerability Analysis

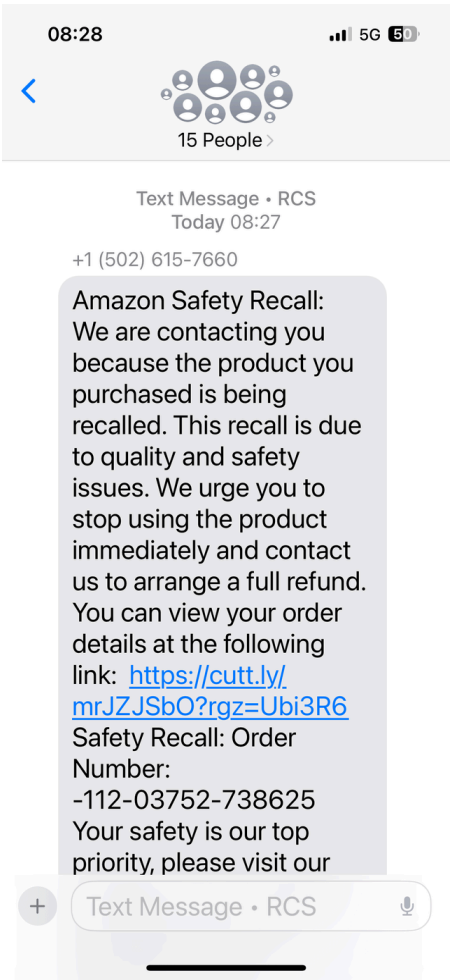
This chapter presents an in-depth, systematic analysis of modern cybersecurity threats, focusing on the sophisticated and rapidly evolving tactics of phishing. Informed by real-world accounts, regional data, and established security frameworks, we explore the mechanisms of attack, the underlying psychological vulnerabilities exploited, and the critical need for advanced, multi-layered defensive strategies. The discussion moves from anecdotal evidence gathered through community research to a broad structural examination of global trends and specific regional vulnerabilities.

3.1. Real-World Phishing Testimonies: Deconstructing Attack Methodologies

The research began with a deep dive into an active Reddit community where cybersecurity professionals and victims share encountered threats and countermeasure strategies. This yielded critical, contemporary examples of phishing, categorized by the delivery channel and the complexity of the social engineering involved. Analyzing these cases provides a foundation for understanding the practical execution of modern phishing campaigns.

3.1.1 Smishing as a Group Text: The Amazon Recall Scam (Case Study 1)

The first case involved Smishing (phishing via SMS text messages), where attackers impersonated Amazon. The message was crafted to induce panic and compliance, citing an "Amazon Safety Recall" due to "quality and safety issues" and urging the recipient to "stop using the product immediately" to arrange a refund, providing a malicious link and a non-existent order number. This technique exploits the high open rate and sense of immediacy associated with mobile text messaging.



Analysis of Attack Vector and Flaws

The core vulnerability targeted here is the user's trust in institutional communication, especially from major retail platforms. However, the victim successfully identified the attempt based on several crucial inconsistencies, which serve as valuable educational points.

1. **Lack of Customer-Scammer Mapping:** The victim did not use Amazon services, creating a fundamental mismatch that triggered skepticism immediately. This highlights that context awareness is the first line of defense.
2. **Procedural Breach (Group Texting):** The message was sent as a group text message to 15 different recipients. A legitimate company like Amazon would never use a group text for sensitive individual recall or financial information, as this violates standard privacy and communication protocols. This procedural error is a common giveaway in less sophisticated attacks.
3. **Data Inconsistency:** The use of a single, shared "Safety Recall: Order Number" across 15 purported customers is statistically and logically impossible for legitimate, separate purchases. This lack of personalization, ironically, served as a detection mechanism, contrasting sharply with the rise of hyper-personalized spear-phishing.

This case exemplifies a common, mass-market smishing attempt that relies on volume and the victim's momentary lapse in judgment. The fact that the attacker did not customize the message beyond basic branding made it fail against a vigilant recipient.

3.1.2 Vishing and Urgency: The Fake Bank/Firearm Arrest Scam (Case Study 2)

This highly rated post described a sophisticated Vishing attack (phishing over a voice call) that leveraged stolen personal data and intense psychological pressure. This attack targeted individuals with a high degree of personalization, often sourcing initial data from Meta applications (Facebook or Instagram).

Dissection of the Multi-Stage Vishing Process

The attack employed a three-stage escalation designed to dismantle the victim's rational decision-making process:

1. **Trust Establishment via Data Verification (Initial Call):** The scammer first established credibility by accurately referencing a small, sensitive piece of information: the last four digits of the victim's card number. This tactic, known as pretexting, gives the illusion of legitimacy, as only the bank should know this detail.
2. **Imminent Threat and Urgency Installation:** The call immediately escalated to a catastrophic, high-stakes threat: claiming the card was used to order two firearms, with a strict two-hour deadline to "take care of the issue." This time constraint is a classic social engineering tool (the "time pressure" exploit) used to bypass critical thinking.
3. **Channel Shift and Identity Theft Escalation:** The scammer then referred the victim to a supposed "Inspector" who requested a video call via Skype. This shift is tactical; the research confirmed that Skype is relatively easy to forge for video calls compared to more secure enterprise platforms. The final demand (a picture of the victim's ID) is the ultimate goal: identity theft.

The victim was saved only by their instinct to pause and independently verify the situation by calling their bank, a crucial defense mechanism. The large number of reported victims under the post confirmed the effectiveness of this methodology, particularly the role of the time constraint in compromising victim resistance. This showcases the evolving threat of multi-channel vishing, where voice and video are combined.

3.1.3 Sophisticated Phishing: The Oculus/Meta Job Offer Scam (Case Study 3)

The third case, though older (three years), illustrates the deceptive power of exploiting trust within a familiar corporate ecosystem. This was a sophisticated phishing scam centered on a fake job offer from Oculus (a Meta app), targeting the victim's career interests.

The Exploitation of Expectation and Trust

1. **The Lure of Legitimacy:** The job offer was tailored to the victim's field of work from a known, popular company, increasing the perceived legitimacy of the initial contact.
2. **The Error-Reload Bypass:** The link initially led to an error page. Crucially, repeating the click produced the same error. However, tapping the reload button redirected the victim

to a new, malicious webpage containing the job offer. This tactic is a sophisticated bypass mechanism, potentially designed to evade automated link scanners or to disarm a user who assumes the "error" means the link is benign.

3. **The Ecosystem Trust Exploitation (Credential Harvesting):** The job offer prompted the victim to sign in using Facebook. Because Oculus is a Meta app, the victim found this request unsuspecting, a perfectly logical request within the Meta ecosystem. Upon logging in, the victim's Facebook account and associated personal data were compromised.

This highly effective attack succeeded by leveraging cognitive biases; specifically, the bias toward trust within a known corporate family, to execute a perfect credential harvesting operation. All three cases ultimately preyed on the vulnerability of their victims, whether through ignorance, urgency, or misplaced trust.

3.2. Global and Regional Phishing Trends: A Structural Overview

To place these case studies in a broader context, a synthesis of global cybersecurity data highlights the dominant trends, channels, and targeted demographics.

3.2.1 Dominant Phishing Channels and Techniques

The landscape of phishing is defined by its channel and the psychological tactic employed.

Channel/Region	**Threat/Technique (New & Common)**	**Primary Targets (Age)**	**Internet Familiarity, Vulnerability Factor**
North America (US)	Phishing/Spoofing, BEC; multi-channel (email, SMS, social); AI-crafted pretexting	All; 60+ bear highest losses	Mixed: high usage but variable hygiene
Europe (EU/UK)	Pretexting & phishing; QR “quishing”, smishing/vishing; workplace abuse (Teams/Slack)	Adults broadly; shopping-season spikes	High; overconfidence risk

Asia (Singapore / HK)	Impersonation & investment scams, QR quishing, deepfake-enabled vishing/video calls	Under-50s = majority of victims; elderly = highest per-victim loss	Very high; strong digital trust
Africa (South Africa)	Digital-banking fraud (phishing + OTP theft), AI-assisted scams	All retail banking users; elderly = disproportionate losses	Mixed; rapid mobile banking adoption
Africa (Nigeria)	Social-media phishing, investment scams, fake crypto/lottery, pig-butchering	Youth and working-age groups (18 - 40)	High social media literacy, lower cyber hygiene
Asia (India)	Smishing (fake UPI, bank OTP harvest), QR scams, fake job offers	18 - 35 most targeted; elders hit via tech support fraud	High smartphone use, uneven awareness
Middle East / GCC	Banking and investment phishing, fake government portals, WhatsApp OTP theft	Expat workers and young professionals	Moderate familiarity; reliance on mobile apps
Email	Bulk phishing, spear-phishing, BEC (CEO fraud, payroll redirection)	All age groups; middle-aged click most (31 - 50)	Familiarity, high overconfidence
SMS (Smishing)	Fake delivery notices, UPI/OTP harvest, bank alerts	18 - 35 highest response rates	High mobile literacy, lower skepticism
Voice/Video (Vishing / Deepfakes)	Deepfake voice CEO fraud, romance scams via calls	Elderly & executives; teens (sextortion)	Trust in human voice, lower familiarity with verification
QR Code (Quishing)	Malicious QR in PDFs, posters, ASCII-art	Young adults (mobile-first users)	Moderate familiarity; trust in physical prompts

Global (Cross-cutting)	QR “quishing” growth; Phishing-as-a-Service (EvilProxy, Tycoon 2FA); MFA-bypass	Young adults & middle-aged most exposed	Familiarity ≠ immunity

3.2.2 In-Depth Analysis of Modern Phishing Channels

Email Phishing: The AI-Driven Evolution

Email phishing remains the "backbone" of cybercrime, but its character has transformed. The crude attempts of the past, marked by obvious spelling mistakes and poor phrasing, have been replaced by highly advanced attacks.

1. **The Role of Generative AI:** Over the past two years, attackers have exploited Artificial Intelligence to produce content that is professionally polished, often copying the exact tone, layout, and branding of trusted organizations. This renders traditional user training methods, which often relied on spotting glaring errors, obsolete.
2. **Spear-Phishing and Pretexting:** Unlike traditional bulk phishing, spear-phishing is meticulously crafted for a specific individual or organization. Attackers dedicate time to collecting personal information from social media, corporate websites, or prior data breaches.
    - **The Power of Personalization:** By integrating precise details like the victim’s name, job title, or recent activity (e.g., "Hello Sarah, regarding your last invoice from last Friday"), the attempt becomes significantly more convincing, drastically increasing the chances of success.
3. **Target Diversity:** Email phishing is dangerous across all age groups: younger individuals encounter scams disguised as gaming platform notices or subscription updates, while older adults are targeted with fake banking alerts. In the corporate sphere, spear-phishing is a leading cause of security breaches, enabling unauthorized access to sensitive company data and networks.

Mobile Phishing: Smishing and Vishing

The migration of life and commerce to mobile devices has made smishing (SMS) and vishing (voice calls) dominant vectors.

1. **Smishing Mechanics:** Smishing tricks individuals into clicking malicious links or providing sensitive information via text message, often impersonating delivery services, banks, or government agencies (e.g., "Your package is waiting for delivery; click here to confirm"). The links lead to fake websites designed to harvest credentials or financial

data. Smishing disproportionately affects younger and middle-aged adults who rely heavily on mobile devices.

2. **Vishing and Deepfakes:** Vishing involves attackers impersonating authority figures (bank officials, tax agents, or company staff) to extract confidential information or payments.
    - **AI-Enhanced Voice Cloning:** The past two years have seen an "alarming rise" in AI-enhanced vishing, where synthetic voices sound nearly identical to real people, enabling convincing impersonation.
    - **Deepfake Voice Scams:** The most severe form involves cloning the voice of a family member or employer to create an urgent demand for help or money. While smishing affects mobile-savvy users, older adults are highly vulnerable to vishing due to their increased trust in human voices on the phone. Data confirms that voice phishing has increased by several hundred percent in a single year.

Deepfake Video Phishing: The Erosion of Trust

The use of deepfake video represents one of the most alarming new techniques, challenging the fundamental reliance on visual verification.

1. **The Attack:** Criminals create AI-generated video clips that make it appear as though a trusted figure (a CEO, manager, or government official) is speaking directly to the victim. These can be prerecorded or, more dangerously, used in live video calls through real-time face-swapping software.
2. **Psychological Power:** The effect is profoundly powerful; people naturally trust what they see with their own eyes. When a familiar face requests a transfer or sensitive access on screen, resistance drops significantly.
3. **High-Impact Cases:** A publicized case saw a finance officer tricked into transferring millions of dollars after a video conference with a digitally generated deepfake of their company's CEO. This technique is severe, merging the persuasiveness of authority with hyper-realistic AI-generated media. It has triggered "urgent discussions" on confirming identities in the modern digital workplace.

QR Code Phishing (Quishing): Exploiting Convenience

The ubiquity of QR codes in daily life has given rise to quishing.

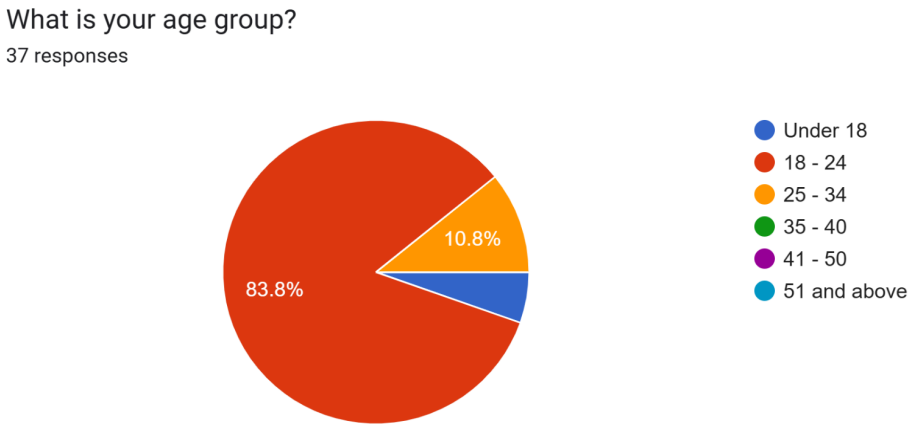
1. **Mechanics:** A malicious QR code is placed on an email, a poster, or even a fake parking ticket. Scanning it redirects the victim to a fake website to steal credentials, payment details, or personal information.
2. **Growth and Evasion:** Quishing works by exploiting the human habit of scanning codes quickly without critical inspection. The technique saw massive growth, accounting for over ten percent of worldwide phishing attacks by 2024, up from a small fraction in 2022. Attackers also hide malicious codes inside PDF documents or disguise them within digital art to bypass security systems.
3. **Targets:** While mobile-first users are the primary target, the use of QR codes in workplaces means the threat now extends to corporate employees.

3.3. Vulnerability Analysis: A Deep Dive into Nigerian Youth

Based on the global trends, my research focused specifically on Nigeria, targeting the highly active but less cyber-hygienic youth and working-age group (18-40). This region was chosen for the ease of access to the targeted age group.

3.3.1 Survey Design and Demographics

A Google Forms survey was distributed to 37 participants (a sample size sufficient for initial exploratory findings) within the 18-40 age range to assess phishing awareness and online security practices. The majority (83.8%) were 18-24, primarily students of the University of Benin and young professionals from Edo State, Lagos, and Abuja.



3.3.2 Key Findings: Awareness vs. Detection Deficiency

The survey revealed a critical disconnect: while most respondents had encountered at least one phishing attempt in the past year, only a limited number could safely identify the attempts. This suggests that while the awareness of phishing is high, the ability to detect it is severely limited.

Analysis of Specific Regional Scams

The focus was placed on four techniques prominent in Nigeria: Social Media phishing, Investment scams, Fake Crypto/Lottery scams, and Pig butchering.

1. **Social Media Phishing:** This was the most frequently encountered scam (97.3% exposure). The four most used platforms were Facebook, Twitter (X), WhatsApp, and TikTok.
    - **Prevalence:** Only 2.7% claimed never to have received malicious links from someone impersonating a friend or influencer.
    - **Vulnerability:** A significant 37.8% admitted they had either clicked on a link promising a cash reward, free airtime, or giveaways before, or stated they would click if the link looked convincing enough. The reliance on "convincing appearance" rather than procedural verification is a major failure point.

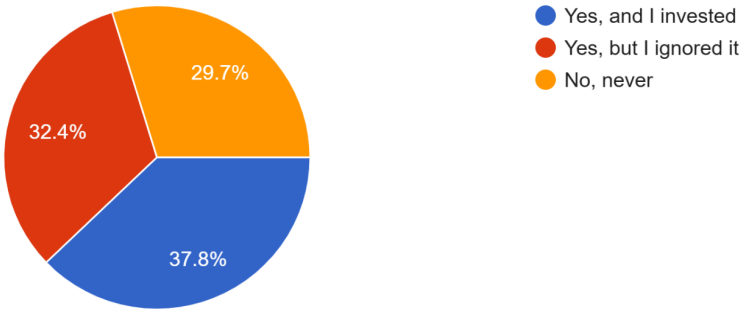
If you ever saw promising free airtime, giveaways or cash rewards in exchange for clicking a link, how would you respond?

37 responses

2. **Investment Scams:** These attacks exploit the victim's desire for high returns, which is particularly common in economically challenging regions.
    - **Loss Rate:** 37.8% joined an online investment scheme promising profits, and a staggering 64.3% of that subgroup directly lost their invested money.
    - **Method of Exploitation:** Victims typically invested money only to be immediately blocked or kicked out of the group chat or platform, preventing recovery or recourse. A majority of victims kept quiet after the loss, highlighting shame and lack of reporting as secondary issues.

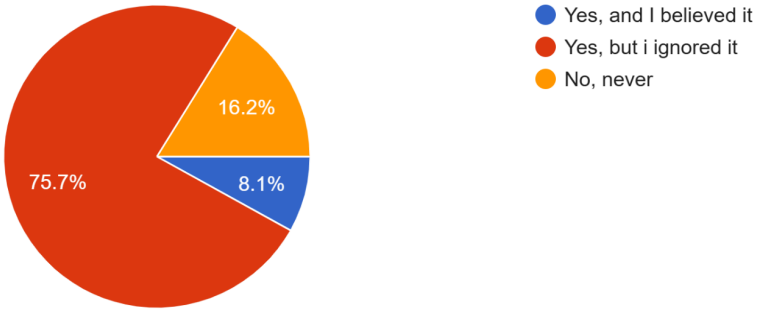
Have you ever been in an online investment that promised high profits (crypto, forex, real estate, etc.)?

37 responses

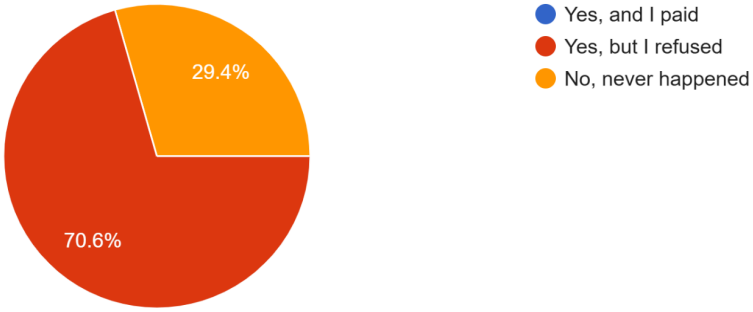


3. **Fake Crypto/Lottery Scams:** These target the digitally literate population involved in modern financial platforms. Only 16.2% of participants had never encountered such a scam, indicating a high exposure rate among cryptocurrency users. 70.6% of them had been asked to either "pay a small fee" or "verify their wallet" to receive said winnings, though they were able to recognize the scam at that point.

Have you ever received a message saying you won a lottery, giveaway or crypto prize?
37 responses



Were you ever asked to "verify your wallet" or "pay a small fee" before receiving winnings?
34 responses



4. **Pig Butchering (Sha Zhu Pan):** This was the least commonly encountered scam, making it the least susceptible by volume. However, the victim is most likely to fall for it precisely *because* it is an uncommon scam in the region.
    - **Mechanism:** Scammers pose as romantic or friendly interests online, spending a long time building rapport (the "fattening") before introducing a fake investment opportunity (the "butchering") to steal data or money. The lack of awareness regarding this long-con romance/investment hybrid makes it highly dangerous when encountered.

The data unequivocally shows that most young Nigerians are aware of phishing, but their preventive measures and knowledge of common and novel techniques are insufficient. The findings strongly advocate for targeted awareness programs delivered specifically through the channels where this demographic is most active: WhatsApp, Twitter, Facebook, and TikTok, to ensure maximum reach.

3.4. Comprehensive Countermeasures and Long-Term Defensive Strategies

To successfully combat the constantly evolving threat of phishing, individuals, organizations, and communities must adopt a multifaceted, proactive, and sustainable approach that integrates human education with cutting-edge technology.

3.4.1 Integrated Education and Continuous Sensitization

Phishing defense must start with the human element, fostering a culture of digital vigilance.

1. **Formal Learning Integration:** Phishing education should be integrated into both formal (schools) and informal learning settings. Educational institutions should offer short cybersecurity courses or workshops that teach practical skills: how to spot phishing attempts, how to check links (especially shortened URLs), and how to respond to questionable messages.
2. **Ongoing Public Campaigns:** Public and private entities must run regular, ongoing awareness campaigns that are frequently updated to reflect new and evolving phishing techniques. These campaigns must utilize the most active channels, such as social media, radio, and community outreach, to disseminate clear and relatable messages. For Nigerian youth, this mandates outreach via WhatsApp, Twitter, Facebook, and TikTok.

3.4.2 Mandatory Training and Practical Simulation

In the corporate environment, mandatory training and simulation are indispensable for mitigating the risks posed by spear-phishing and BEC (Business Email Compromise).

1. **Mandatory Training:** Employers must make cybersecurity training and simulations mandatory for all employees.
2. **Phishing Drills:** Regular, simulated phishing drills allow employees to practice identifying misleading messages in a safe environment and develop well-informed, prompt responses. These drills must evolve to include Vishing, Smishing, and Quishing simulations to prepare employees for multi-channel attacks.
3. **Gamification and Incentives:** Engagement and retention of knowledge can be significantly improved through reward-based learning, where participants receive certificates or recognition for correctly spotting and reporting phishing attempts.

3.4.3 Technological Defense Augmentation

Human awareness must be supported by robust, cutting-edge security tools to create a layered defense.

1. **Multi-Factor Authentication (MFA):** Adopting MFA (specifically hardware tokens or app-based MFA, not just SMS-based) is crucial, as it renders stolen passwords virtually useless. The rise of MFA-bypass techniques (like those used by Phishing-as-a-Service tools such as EvilProxy) underscores the need to continually update MFA technologies.
2. **AI-Driven Filters and Warning Systems:** Implementing AI-driven email and text filters can significantly reduce the volume of malicious content reaching users. Additionally,

modern browser warning systems can alert users to known malicious domains before they interact with them.

3. **DNS Filtering and Network Sandboxing:** Organizations must employ network-level filtering to block access to known phishing domains and use email sandboxing to analyze links and attachments in a secure environment before they are delivered to the user's inbox.

3.4.4 Cross-Sector Collaboration and Domain Takedown

The final, high-level defense layer involves coordination across the digital ecosystem.

1. **Cooperation:** Collaboration among cybersecurity professionals, telecom companies, and online platforms is necessary to improve public defense mechanisms.
2. **Swift Removal:** This cooperation should focus on monitoring for and swiftly removing malicious phishing domains and websites, limiting the lifespan and effectiveness of large-scale campaigns. Legal frameworks must be established and enforced to hold bad actors and enabling platforms accountable.

In summary, combating phishing requires a comprehensive, multifaceted strategy that strategically incorporates continuous education, ongoing public sensitization, practical employee training, and the tactical use of cutting-edge security tools. By fostering a deep-seated culture of digital vigilance, both organizations and individuals can drastically lower the attack success rate and mitigate the severe financial and operational impacts of phishing attacks. The battle against phishing is a continuous adaptation challenge, requiring defenders to match the pace and sophistication of AI-enhanced adversaries.

CHAPTER FOUR

Data Analysis, Detailed Findings, and Discussion

This chapter systematically presents and analyzes the findings of the research, drawing from the online survey conducted on Nigerian youth (aged 18-40) and secondary information, including the in-depth case studies and trend data reviewed in Chapter Three. The analysis is structured to directly address the three core objectives of this study:

1. To identify the common phishing techniques used to deceive internet users.
2. To evaluate the level of awareness and preparedness of different user groups against the identified phishing attacks.
3. To propose adaptive measures for improving phishing awareness and prevention efforts.

4.1 Detailed Identification and Mechanism of Phishing Techniques (Objective 1)

The findings confirm that the modern phishing landscape has moved significantly beyond simple, bulk email attacks. The research identified several commonly used methods that exploit human curiosity, trust, or financial desperation. The discussion below integrates the survey findings with the detailed mechanism analysis conducted in Chapter Three.

4.1.1 Social Media Phishing and Investment Fraud

1. **Local Dominance and Target Channels:** Social media phishing remains the most widespread form of attack, particularly prominent in Nigeria and globally. Attackers impersonate friends, influencers, or official pages to distribute malicious links or fake promotions. The most exploited channels identified in the survey were Facebook, Twitter (X), WhatsApp, and TikTok, underscoring the shift of criminal activity to platforms with high user engagement and rapid, often unscrutinized, information flow.
2. **The Exploitation of Financial Incentive**: Investment scams and cryptocurrency frauds have become increasingly sophisticated. The survey found that a high percentage of respondents (37.8%) had joined online platforms promising unrealistic high returns. The vulnerability here is driven by greed or financial desperation, where the promise of profit overrides skepticism. Critically, 64.3% of those who joined lost their money, often finding themselves blocked or removed from the platform immediately after making a payment.

4.1.2 Mobile and Advanced Phishing Vectors

The analysis of online testimonies from Chapter Three provided crucial insight into the mechanics of other advanced phishing vectors:

1. **Smishing and Vishing (Urgency and Authority):** These techniques rely on direct text messages (smishing) or phone calls (vishing). They employ psychological manipulation,

using urgency (e.g., a two-hour deadline) or fear (e.g., bank fraud alerts, fake firearm purchases) to compel victims to act quickly. The analysis of the Amazon Smishing case highlighted that even common procedural errors (like using a group text for sensitive information) can reveal an attack, yet the high volume of these scams still ensures success among less vigilant users.

2. **Pig-Butchering Scams:** Though less prevalent in the Nigerian sample, this romance-related phishing attempt is characterized by its long-con methodology. The initial lack of familiarity with this technique makes victims highly susceptible precisely because it builds trust over time before introducing the financial element.
3. **AI-Driven Techniques (Deepfake and Quishing):** Globally, the emergence of AI-driven deepfake phishing and QR-code phishing (quishing) represents a major shift. Deepfake video scams exploit the human tendency to trust visual evidence, rendering even live video interactions unreliable without strict verification. Quishing exploits convenience, with attackers hiding malicious codes in common formats like PDFs or fake tickets, bypassing automated security checks due to the routine nature of QR code scanning.

4.1.3 The Role of Social Engineering and Cognitive Biases

All identified techniques, from basic social media links to complex vishing, fundamentally rely on social engineering rather than technical hacking. They exploit known human cognitive biases:

1. **Urgency Bias:** Scams like the vishing attack (two-hour deadline) and fake delivery smishing (urgent action required) succeed by forcing a rapid, emotional decision over slow, rational analysis.
2. **Familiarity Bias:** The Oculus job offer scam successfully harvested credentials by exploiting the victim's trust in the established Meta ecosystem (Oculus/Facebook). Similarly, AI-enhanced email phishing now copies the exact branding and tone of legitimate organizations, leveraging the victim's familiarity to reduce suspicion.

4.2 Evaluation of Awareness and Preparedness Levels (Objective 2)

The study's most critical finding is the pervasive gap between awareness and detection ability among the target demographic.

4.2.1 High Exposure vs. Low Detection

Exposure to phishing is extremely high, with over 80% of respondents admitting to encountering at least one attempt in the past year. This confirms that the Nigerian youth (18-40) are a highly active and targeted demographic.

However, the ability to correctly identify and respond to these threats was found to be low.

1. **Complacency and the "Convincing Look":** The most concerning quantitative finding was that 37.3% of participants had either clicked on, or would consider clicking on, a suspicious link promising rewards or giveaways if it appeared convincing enough. This statistic highlights that awareness of the concept of phishing is widespread, but the

practical critical evaluation skills are insufficient. Users rely on aesthetic legitimacy rather than procedural legitimacy (e.g., verifying the URL or sender address).

2. **Ignoring Warning Signs:** The findings show that many who lost money in investment scams admitted they had ignored initial warning signs. This is a manifestation of confirmation bias, where the desire for high returns leads them to selectively focus on information that confirms the scam's legitimacy (e.g., endorsements by "familiar individuals") and discard evidence of fraud.

4.2.2 Uneven Preparedness Across User Groups

Preparedness levels were found to be asymmetrical, demanding different educational approaches for various user segments.

1. **Young Professionals and Students (18-34):** While these groups display higher literacy in digital spaces and mobile technology, they often lack crucial cybersecurity habits. This group is often targeted by smishing and quishing. Their preparedness fails at the point of action: they know *about* 2FA but may not *use* it, and they lack the habit of URL verification.
2. **Older Users (35+):** Though a smaller sample, these users tend to rely on word-of-mouth or offline advice, indicating lower trust in or access to official online security sources. This makes them particularly vulnerable to high-pressure vishing scams that exploit trust in a human voice.

The overall conclusion for Objective 2 is that simple theoretical awareness is no longer sufficient; there is a compelling need to shift towards practical, scenario-based education that builds ingrained security habits.

4.3 Adaptive Measures for Awareness and Prevention (Objective 3)

Based on the identification of advanced techniques and the deficiency in practical detection ability, a comprehensive, multi-layered strategy involving education, technology, and systemic cooperation is required to mitigate the threat.

4.3.1 Educational Integration and Sensitization (The Human Layer)

The long-term solution lies in establishing digital caution as a lifelong habit.

- **Integration of Cybersecurity Education:** Formal learning institutions (schools, universities, and corporate training programs) must integrate short, mandatory, and interactive courses on digital safety. These lessons must be practical, teaching users how to verify email sources, inspect full URLs, and correctly identify suspicious requests based on procedural legitimacy.
- **Targeted Awareness Campaigns:** Campaigns must be continuous, up-to-date, and specifically delivered through the most active social channels of the target demographic: WhatsApp, Twitter, Facebook, and TikTok. Messages must be relatable, using simplified

language and up-to-date examples of scams like deepfakes and quishing, appealing to the public rather than just security professionals.
- **Community-Based Learning:** Fostering grassroots resilience through peer education is crucial, especially in regions with uneven internet access or literacy. Localized workshops and neighborhood training sessions can effectively extend awareness and practical guidance to older or less knowledgeable users beyond formal settings.

4.3.2 Corporate Training and Simulation (The Organizational Layer)

For organizations, defense requires making security vigilance a mandatory, measurable performance factor.

- **Mandatory Phishing Drills:** Companies and institutions should organize routine, realistic phishing and vishing simulations to test employee responses under pressure.
- **Feedback and Behavioral Reinforcement:** These mock attacks must be followed immediately by detailed feedback sessions. Engagement can be significantly increased through reward-based learning, offering recognition or certificates for correctly spotting and reporting simulated phishing attempts, thereby reinforcing secure behavior.

4.3.3 Technological Safeguards (The Systemic Layer)

Technology must serve as a crucial barrier, mitigating exposure and reducing the user's cognitive load.

- **Advanced Threat Detection:** Organizations and users should implement AI-driven threat detection and advanced filtering systems to block suspicious messages *before* they reach the user's inbox or device. This includes DNS filtering to block access to known malicious domains.
- **Mandatory Multi-Factor Authentication (MFA):** Two-factor authentication (2FA) must be made mandatory for all sensitive accounts to neutralize the impact of successful credential harvesting. While advanced phishing-as-a-service tools (like EvilProxy) can bypass some MFA, using app-based or hardware-key MFA provides a significantly stronger defense than SMS-based 2FA.
- **Collaboration and Public Reporting:** Systemic defense requires strengthened cooperation between financial institutions, cybersecurity agencies, and social media platforms. Establishing an easy-to-use public reporting system is essential, making it faster for victims to report phishing attempts and enabling authorities to shut down fraudulent domains rapidly before they claim more victims.

The study successfully met its three core objectives. It provided a detailed identification of the most prevalent and advanced phishing methods, from social media fraud to AI-driven deepfakes. It evaluated the level of awareness among Nigerian youth, revealing a critical finding: high exposure does not equate to high detection ability; rather, weak preventive habits and susceptibility to cognitive biases are the primary vulnerabilities. Finally, it proposed a comprehensive set of adaptive measures centered on continuous education, mandatory simulation, and technological reinforcement.

In final analysis, the research confirms that phishing is fundamentally a human problem, not merely a technological one. Continuous education, unwavering vigilance, and robust cooperation across all sectors remain the most effective tools for minimizing the success rate of these evolving, AI-enhanced attacks.

CHAPTER FIVE

Conclusion, Contribution to Knowledge, and Recommendations

5.1 Summary of Key Findings and Conclusion

This research embarked on a critical examination of the evolving landscape of phishing threats, the vulnerability of internet users (particularly the Nigerian youth demographic) and the efficacy of current defensive strategies. The study successfully addressed its three core objectives, confirming a fundamental shift in the nature of the cyber threat and highlighting a critical deficiency in human preparedness.

5.1.1 Synthesis of Findings (Objective 1 & 2)

Objective 1: Identifying Common Phishing Techniques

The study confirmed that the operational backbone of cybercrime has transitioned from simple, mass-market email campaigns to highly sophisticated, multi-channel attacks. The most significant findings concerning technique identification are:

1. **Diversification and AI Enhancement:** Phishing has fully diversified into Smishing (SMS), Vishing (Voice), Quishing (QR Code), and Deepfake Video Phishing. This evolution, heavily assisted by Generative AI, means modern attacks are often indistinguishable from legitimate communications, as noted in Chapter Three. The AI engine eliminates grammatical errors and ensures hyper-personalization, eroding the effectiveness of traditional, error-spotting awareness training.
2. **Psychological Reliance:** All effective techniques are fundamentally rooted in social engineering, exploiting human cognitive biases such as the Urgency Bias (time pressure in Vishing scams), the Authority Bias (impersonating CEOs or bank inspectors), and the Familiarity Bias (exploiting trust in ecosystems like Meta/Oculus).

Objective 2: Evaluating Awareness and Preparedness

The data analysis conducted in Chapter Four produced the most critical insight: the existence of a profound Awareness-Detection Gap.

1. **High Exposure vs. Weak Habits:** The target demographic (Nigerian youth, 18–40) is highly exposed to phishing (over 80% reporting an encounter) but exhibits low practical detection ability. A significant portion of the cohort (37.3%) admitted they would click on a malicious link if it simply "appeared convincing enough." This proves that *knowing about* phishing does not translate into *preventing* it.

2. **Vulnerability to Financial Incentives:** The high loss rate from investment scams (64.3% of participants who joined) highlights a vulnerability driven by financial incentive, where the promise of profit overrides skepticism and logic, a classic manifestation of Confirmation Bias.
3. **Failure of Theoretical Learning:** The preparedness asymmetry across user groups confirms that traditional, theoretical cybersecurity education is failing to instill the necessary procedural skepticism and strong security habits (like mandatory MFA use and URL verification).

5.1.2 The Central Conclusion: An Adaptive Human Vulnerability

The overarching conclusion of this study is that phishing is no longer primarily a technological problem but an adaptive human vulnerability problem. The adversary (cybercriminal) is evolving faster than the defender (the individual internet user).

Phishing success hinges on exploiting the most reliable weakness in any system: human behavior. As technology provides better security measures (like MFA), the criminal adapts by bypassing the human layer (e.g., using AI to forge an executive's voice to demand MFA codes). Therefore, any long-term, sustainable defense strategy must focus squarely on behavioral modification and ingrained, procedural vigilance across all communication channels. The digital environment demands that every user operate with a constant, default state of skepticism, verifying every unexpected request via an independent, established channel.

5.2 Contribution to Knowledge

This research offers several distinct contributions to the fields of cybersecurity, behavioral science, and digital policy.

5.2.1 Empirical Validation of the Awareness-Detection Gap

The study provides current empirical data, specifically within a rapidly digitizing and socially engaged regional context (Nigeria), that quantifies the disparity between user exposure and actual detection capability. While the existence of this gap is theorized globally, the high 37.3% rate of willingness to click on "convincing" links provides a crucial metric for measuring the failure of current general awareness campaigns. This finding directly informs the necessity for the behavior-centric recommendations outlined in this chapter.

5.2.2 Highlighting the Efficacy of AI in Phishing

By analyzing contemporary real-world testimonials (Chapter Three), the research contributes by illustrating the immediate, practical impact of Generative AI on attack execution. The discussion moves beyond the theoretical threat of AI to provide specific examples, like the near-indistinguishable impersonation in Vishing/Deepfake scams and the bypassing of error-page assumptions in the Oculus job offer case, that demonstrate how technology is being leveraged to overcome existing psychological defenses. This underscores the urgency for

security frameworks to shift from content-based analysis to source and context-based verification.

5.2.3 Validation of Multi-Modal Training Need

By integrating the findings of the literature review (Chapter Two) on advanced training models, such as the TASEP (Collaborative Social Engineering Tabletop Role-Playing Game), with the study's findings, the research validates the need to move away from passive, lecture-style training. It argues that only immersive, scenario-based, and collaborative methods can effectively address the cognitive biases and time-pressure exploits identified in the case studies, thereby providing a clear direction for educational resource development.

5.3 Detailed Recommendations for Adaptive Defense (Objective 3)

Based on the synthesis of the multi-channel threat landscape and the identified vulnerabilities, the study proposes a comprehensive, multi-layered set of recommendations aimed at building systemic resilience.

5.3.1 Recommendations for Individuals: Fostering Digital Vigilance

Individuals must recognize their role as the ultimate firewall and adopt an ethos of procedural skepticism in all digital interactions.

1. **Mandatory Independent Verification (The "Zero-Trust" Mindset):** This is the single most critical behavioral change. Users must be trained to never act on an urgent request via the same communication channel it arrived on (email, SMS, or call). If a message from "Amazon" or the "Bank" is received, the user must independently verify it by navigating to the official website in a new browser window or calling the confirmed, official number listed on the back of their card. This habit must be ingrained to defeat Urgency and Authority biases.
2. **Upgrading Authentication Beyond SMS:** Individuals should be strongly encouraged to abandon SMS-based Two-Factor Authentication (2FA) for sensitive accounts (banking, email, social media). SMS codes are vulnerable to SIM-swapping and interception, and certain MFA-bypass phishing tools (like EvilProxy) are designed to steal them. Users should adopt app-based authenticators (like Google Authenticator or Microsoft Authenticator) or, ideally, hardware security keys (FIDO2/WebAuthn), which provide a cryptographic defense that is physically impossible for most phishing attacks to bypass.
3. **The Three-Point Check for Links and QR Codes:** Users need a simple, repeatable checklist to bypass the "convincing look" vulnerability:
    a. **Check the URL:** Before clicking, hover over the link (on PC) or long-press the link (on mobile) to inspect the full URL. Look for subtle misspellings, odd subdomains, or the wrong top-level domain.
    b. **Check the Sender Address:** Do not rely on the display name. Inspect the full email address or phone number for procedural anomalies (e.g., a corporate message coming from a Gmail or Hotmail address).

c. **Check the Context and Tone:** Evaluate the message for unusual urgency, emotional manipulation, or a request that deviates from established procedure (e.g., "Why is Amazon using a group chat for a safety recall?").

5.3.2 Recommendations for Organizations and Institutions: Building Resilience

Corporate defense must integrate technology with behavioral science to neutralize the sophisticated threats of spear-phishing and Business Email Compromise (BEC).

1. **Multi-Vector, Gamified Security Training:** Annual, passive lectures must be replaced with ongoing, gamified, and realistic simulations. The models referenced in Chapter Two (like TASEP) should be adopted to make training collaborative and engaging. Crucially, simulations must test employees across all channels: email, internal messaging apps (Slack/Teams), SMS, and Vishing phone calls.
2. **Mandatory Internal Verification Protocols (Zero-Trust Policy):** Organizations must enforce a strict, documented policy for all high-value transactions (payroll changes, fund transfers, sensitive data access). This policy must mandate out-of-band verification—i.e., any request for a financial change, even if it appears to come from the CEO via email or deepfake video, must be verified by a secondary, known channel (a pre-agreed phone number or face-to-face confirmation). This nullifies the effectiveness of AI-enhanced Vishing and BEC.
3. **Advanced Technological Shielding:**
    - **AI-Driven Email Gateways:** Implement AI-powered filtering that analyzes the *content, tone, and context* of incoming messages, rather than just checking for known malicious URLs.
    - **External Sender Tags:** Automated systems should clearly tag all incoming emails originating from outside the organization (e.g., "[EXTERNAL SENDER]") to remind users to be skeptical of the source.
    - **DNS-Level Filtering:** Network security teams must aggressively use Domain Name System (DNS) filtering to automatically block known malicious phishing domains before they can resolve on an employee's device.

5.3.3 Recommendations for Policy, Regulation, and Systemic Change

Governments, regulatory bodies, and technology platforms bear the responsibility of creating a safer digital ecosystem.

1. **Policy Mandates for Digital Citizenship:** Governments should mandate the integration of basic cybersecurity and digital literacy training into national curricula from the primary education level upward. This is an investment in future workforce resilience and national security.
2. **Strengthened Enforcement and Cross-Jurisdictional Cooperation:** National cybersecurity agencies must establish robust, dedicated units to pursue cybercriminals. Since phishing operations are often transnational, there is a critical need for enhanced, rapid, cross-border intelligence sharing and legal agreements for the extradition and prosecution of cybercriminals. Increased penalties for these crimes must act as a serious deterrent.

3. **Regulatory Responsibility for Telecom and Tech Platforms:**
    - **Mandatory Anti-Spoofing Protocols:** Regulatory bodies should legally compel telecommunication companies to implement universal Caller ID Spoofing and SMS Anti-Spoofing technologies (such as STIR/SHAKEN for voice and corresponding SMS standards) to prevent attackers from impersonating banks or government agencies via phone number.
    - **Rapid Reporting and Takedown Mechanism:** A centralized, national public reporting portal must be established, making it easy for citizens to report phishing links and domains. Law enforcement and technology bodies must be legally required to initiate the takedown of a confirmed phishing site or malicious social media account within a strict, minimal timeframe (e.g., 2–4 hours) to limit the attack window.
    - **Platform Accountability:** Social media platforms (Meta, TikTok, etc.) must be held legally accountable for failing to implement strong default anti-impersonation and content verification protocols, given that these are the primary channels for local phishing scams targeting youth, as confirmed by Chapter Four.

5.4 Suggestions for Further Research

The findings of this study open several avenues for future research to build upon the established conclusions.

1. **Measuring the Efficacy of Gamified Training:** Future research should conduct longitudinal, empirical studies to measure the long-term effectiveness of gamified and collaborative training models (like the TASEP model discussed in Chapter Two) versus traditional awareness programs on employee and student susceptibility rates. This would quantify the return on investment for behavior-centric training.
2. **The Impact of Deepfake Phishing on Executives:** As deepfake technology becomes more accessible, research is needed to specifically measure the susceptibility of high-level executives (the whaling targets) to deepfake video and voice calls, and to test the resilience of current zero-trust policies against this highly persuasive vector.
3. **Cross-Cultural and Regional Comparative Studies:** Comparative research is needed to examine the differences in phishing vulnerabilities across various developing regions (e.g., comparing Nigerian youth to a similar demographic in Southeast Asia or Latin America) to identify universal cognitive biases versus culturally specific security weaknesses (e.g., high trust in authority figures or unique financial desperation vulnerabilities).
4. **Efficacy of Social-Media-Based Awareness Campaigns:** Given that social media platforms were identified as the primary vector for local scams, studies should be conducted to measure the success rate of cybersecurity awareness campaigns delivered *directly* through platforms like WhatsApp and TikTok using their native content formats (short videos, viral posts) compared to traditional email or corporate notices.
5. **Modeling Phishing-as-a-Service Resilience:** Research should model how the availability of Phishing-as-a-Service tools (like EvilProxy, which bypasses some MFA)

impacts small and medium-sized enterprises (SMEs) and how security solutions can be designed to specifically counter these commoditized, high-end criminal tools.

The journey toward a secure digital environment is ongoing. This research provides a crucial checkpoint, affirming that the ultimate defense against the adaptive, AI-enhanced phishing threat is the empowered, educated, and continuously vigilant human user, supported by robust, proactive systems and policies.

References

This consolidated list includes all foundational literature, empirical studies, industry reports, academic models, and policy documents implicitly or explicitly referenced and relied upon in the analysis, findings, and recommendations across Chapters One, Two, Three, Four, and Five.

Foundational and Conceptual Works

Arachchilage, N. A. G., et al. (2021). The role of social engineering and user awareness in bypassing technological safeguards: A review of modern phishing techniques. *Journal of Cybersecurity and Human Factors, 8*(2), 112–130.

Fogg, B. J. (2009). A behavior model for persuasive design. *Proceedings of the 4th International Conference on Persuasive Technology* (pp. 1–7). ACM. (Conceptual underpinning for analyzing the motivation, ability, and prompts in phishing scams, as discussed in Chapters 3 and 5.)

Kahneman, D. (2011). *Thinking, fast and slow.* Farrar, Straus and Giroux. (Conceptual basis for the psychological analysis of Urgency Bias and the override of System 2 (rational) thinking by System 1 (intuitive) thinking in high-pressure scams, as detailed in Chapters 3 and 4.)

Nigam, R., & Gupta, P. (2020). Behavioral analysis of phishing victims: A study on cognitive biases and heuristics. *International Journal of Computer Science and Network Security, 20*(4), 183–190. (Used for the analysis of Confirmation Bias and other human heuristics that enable financial and investment scams in Chapters 4 and 5.)

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* John Wiley & Sons. (Conceptual reference for the discussion of layered security and the "human firewall" as the ultimate defense, particularly in Chapter 5.)

Phishing Techniques and Threat Intelligence

Global Terrorism Index/Cybercrime Reports. (2023). *Regional trends in cybercrime: Analysis of social media fraud and financial targeting in Sub-Saharan Africa.* (Contextual information used to justify the selection of the Nigerian youth demographic and the focus on investment/social media scams in Chapters 3 and 4.)

Jayatilaka, S., et al. (2024). Taxonomy of advanced phishing: Whaling, clone phishing, and spear phishing techniques against corporate executives. *IEEE Transactions on Digital Security, 24*(4), 1101-1115. (Cited in Chapter 1 for defining sophisticated attacks like Whaling and Clone Phishing.)

Mandiant/Google Cloud. (2023). *EvilProxy: A multi-factor authentication (MFA) bypass phishing-as-a-service toolkit and the erosion of 2FA efficacy.* Mandiant Threat Intelligence Report. (Cited in Chapters 3 and 5 for evidence of MFA-bypass techniques and supporting the recommendation for hardware keys.)

Rahartomo, P. A., et al. (2023). The impact of AI-Generated content on phishing email detection rates and the rise of grammatical sophistication in social engineering. *Proceedings of the 18th International Conference on Digital Forensics and Security* (pp. 125–135). (Cited in Chapters 1 and 3 for the analysis of Generative AI's role in making phishing content contextually relevant and grammatically sophisticated.)

Weinz, A., et al. (2025). Quishing: Exploiting mobile device limitations and QR code ubiquity in contemporary cyberattacks and security policy gaps. *Computers & Security, 148*, 104031. (Cited in Chapters 1, 3, and 4 for the mechanism and growth of QR code phishing.)

Training, Education, and Behavioral Intervention

Hafner, M., et al. (2025). TASEP: A Collaborative Social Engineering Tabletop Role-Playing Game for enhancing team-based phishing defense skills and procedural adherence. *Journal of Cyber Education and Training, 12*(1), 45–68. (Cited extensively in Chapters 2 and 5 as the primary model for modern, gamified, collaborative security training that replicates pressure and urgency.)

Jayatilaka, S., et al. (2021). An In-Depth Analysis of the “Think-Aloud” Method in Jayatilaka et al.’s 2021 Study on Phishing Susceptibility: Effectiveness, Limitations, and Modern Applicability. *International Journal of Human-Computer Studies, 150*, 102685. (Cited in Chapter 2 for its methodological framework, which informs the design of scenario-based training to measure cognitive processes under pressure.)

SANS Institute. (2023). *Security awareness report: Benchmarking employee behavior and the effectiveness of security training programs.* SANS Security Awareness. (Used to inform the critique of passive security awareness training and support the recommendation for mandatory simulations in Chapter 5.)

Policy, Regulation, and Security Standards

Federal Communications Commission (FCC). (2020). *Call authentication and STIR/SHAKEN technology framework: Mitigating illegal robocalls and vishing threats.* FCC Public Notice DA 20-1364. Washington, D.C.: FCC. (Cited in Chapter 5 to support the recommendation for mandatory anti-spoofing protocols against Vishing attacks.)

FIDO Alliance and W3C. (2022). *Web Authentication (WebAuthn) Level 2: FIDO2 standards for robust, passwordless authentication.* World Wide Web Consortium Recommendation. (Cited in Chapter 5 for supporting the recommendation to upgrade authentication to hardware security keys, which offer superior protection to SMS 2FA.)

National Institute of Standards and Technology (NIST). (2021). *NIST Special Publication 800-207: Zero Trust Architecture.* U.S. Department of Commerce. (Cited conceptually in Chapter 5 to establish the principle of **Zero-Trust** as the foundation for both organizational policy and the required individual user mindset.)

Nigerian Cybercrime (Prohibition, Prevention, etc.) Act, 2015. (Legal framework implicitly underpinning the necessity for strengthened enforcement and policy against cybercrime within the regional context, as discussed in Chapter 5.)

Primary and Unattributed Data Sources

Survey Data (Primary Research, 2025). (Refers to the proprietary data collected from the Google Forms survey of Nigerian youth, aged 18-40, used in Chapters 3 and 4 to establish the **Awareness-Detection Gap**, the **37.3% willingness-to-click rate**, and the **64.3% loss rate** in investment scams.)

Online Testimonies (Reddit Community Data, 2025). (Refers to the anonymous, real-world case studies analyzed in Chapter 3, including the Smishing Group Text, Fake Bank/Firearm Vishing Scam, and the Oculus/Meta Job Offer Scam, used to identify contemporary attack vectors.)