UNIABUJA Journal of Engineering and Technology

https://ujet.uniabuja.edu.ng/

ISSN: 2714-3236 (Online); 2714-3228 (Print)

Volume 2, Issue 2, 2025; 469-481

Assessing Human Vulnerabilities and Social Engineering Threats in Web-Based School Management Systems for Junior Secondary Schools in the Federal Capital Territory

Ibrahim H. BISALLAH[1], Shuaibu M. ISAH[2], Fatimah B. ABDULLAHI[3], Christopher U. EBELOGU[4*]

[1,2,3,4*]*Department of Computer Science, University of Abuja, Abuja, Nigeria*

[1]*hashim.bisallah@uniabuja.edu.ng*, [2]*shuaibuis@gmail.com*, [3]*fatimah.abdullahi@uniabuja.edu.ng*, [4*]*ebelogu.chris@uniabuja.edu.ng*

Abstract

The adoption of Web-Based School Management Systems in FCT UBEB Junior Secondary Schools has greatly improved administrative efficiency. However, their implementation has also revealed cybersecurity vulnerabilities, especially social engineering. Social engineering weakens technical security measures by manipulating human psychology. This paper explores human-related vulnerabilities that increase social engineering risks in SMS Web-Based Management Systems in schools. It addresses issues like low cybersecurity awareness, weak passwords, and susceptibility to phishing. These vulnerabilities and existing security measures are analyzed through surveys, interviews, and system audits. Results indicate that over 70% of students and staff are unable to recognize phishing emails, and password reuse is a common practice. Additional risks include limited use of multi-factor authentication and outdated antivirus software. Social engineering attacks can lead to data breaches, financial losses, and damage to the institution's reputation and operational stability. Consequently, the study proposes a Human-Centric Social Engineering Mitigation Framework (HC-SEMF) that integrates user awareness training, behavioral analysis, and technical security controls to enhance the resilience of Web-Based School Management Systems in junior secondary schools.

Keywords: *Social Engineering, Cybersecurity Awareness, Phishing Attacks, Human Vulnerabilities, Web-Based School Management Systems.*

1.0 Introduction

Social engineering attacks have increased in frequency and sophistication, and vulnerabilities related to people have grown significantly in importance (Ahmed et al., 2020). According to Klein et al. (2019), social engineering attacks leverage human vulnerabilities, such as psychological manipulation, to obtain unauthorized access to systems or data. Serious repercussions from these attacks may include data breaches, monetary losses, and reputational harm (Bullee et al., 2020).

The education sector is especially susceptible to social engineering attacks because of the sensitive information stored within school management systems. Personal details of students and staff, financial data, and academic records are all potential targets for attackers (Liu et al., 2019). Moreover, the education sector is often characterized by a lack of resources and expertise, making it difficult for schools to implement effective security measures (Bullee et al., 2020).

Web-based School Management Systems are particularly vulnerable to social engineering attacks due to their open-source nature and the lack of security features in many web applications (Zhao and Gong 2015). The widespread use of web-based development has made it a popular target for attackers, with many vulnerabilities being discovered in web-based applications in recent years (Zhao and Gong 2015).

Social engineering attacks on school management systems can take many forms, including phishing attacks, pretexting, and baiting (Krombholz et al., 2015). Phishing attacks involve tricking individuals into divulging sensitive information, such as login credentials or financial information, through fraudulent emails or websites (Dhamija et al., 2006). Pretexting involves creating a fake scenario or story to gain an individual's trust and obtain sensitive information (Klein et al., 2019). Baiting involves leaving a malware-infected device or storage media, such as a USB drive, in a public area for an individual to find and plug into their device (Krombholz et al., 2015).

The impact of social engineering attacks on school management systems can be profound, leading to data breaches, financial losses, and damage to reputation (Bullee et al., 2020). A data breach may cause the unauthorized disclosure of sensitive information belonging to students and staff, including personal and financial details (Liu et al., 2019). Financial losses could stem from the theft of financial data or the interruption of financial transactions (Bullee et al., 2020). Reputational damage can result from negative publicity and loss of trust in the school and its management (Liu et al., 2019).

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

Thus, looking into the effects of social engineering attacks on Web-Based School Management Systems for FCT junior secondary schools and human-related vulnerabilities in these systems is imperative. This study aims to identify the human-related vulnerabilities in Web-Based School Management Systems, investigate the impact of social engineering attacks on these systems, and propose recommendations for mitigating the risk of social engineering attacks on school management systems.

However, this technological advancement also introduces a concomitant risk landscape. The sensitive nature of data stored within School Management Systems, such as student records, attendance data, and communication logs, makes them attractive targets for cyberattacks. As the FCT UBEB Junior Secondary Schools continue their efforts toward digitization, they encounter the challenge of safeguarding sensitive information in the face of increasingly sophisticated cyber threats (Atuh et al., 2023).

One subset of these threats that demands particular attention is social engineering attacks. Social engineering leverages human psychology and manipulation to exploit individuals into divulging confidential information, performing actions that compromise security, or unknowingly granting unauthorized access (Nas et al., 2024). While technical vulnerabilities in software can be addressed through coding practices and software updates, human-related vulnerabilities remain a persistent challenge. Cybercriminals adept at social engineering can often bypass technological barriers by exploiting human behavior, including trust, curiosity, and lack of awareness (Nas et al., 2024).

This study addresses the existing knowledge gap concerning human-related vulnerabilities in Web-Based School Management Systems used by FCT UBEB Junior Secondary Schools. By focusing on social engineering attacks, it empirically examines the interaction between human behavior and technological controls to identify exploitable weaknesses within these systems. The study further contributes by providing context-specific evidence and proposing targeted mitigation strategies to enhance the cybersecurity resilience of school management systems (Alexander, 2016).

2.0 Literature Review

Social engineering attacks can incorporate elements from various categories, including human, computer, technical, social, and physical methods. Examples of these attacks include phishing, shoulder surfing, impersonation during help desk interactions, baiting, theft of important documents, diversion theft, dumpster diving, fake software, robocalls, quid pro quo schemes, pretexting, tailgating, deceptive pop-up windows, ransomware, online social engineering, reverse social engineering, and phone-based attacks.

Alghamdi (2025) points out that social engineering remains a constant cybersecurity threat, worsened by AI and deepfake technologies. He emphasizes the need for technical defenses along with user training. One drawback is the absence of real-world proof for the suggested strategies. Similarly, Okeke and Amaechi (2024) examine phishing in higher education. They identify weaknesses from email, spear, and AI-driven attacks and call for combined awareness programs and technical measures like machine learning and multi-factor authentication. However, their analysis relies on literature and lacks practical evidence to support its effectiveness.

According to Martins (2023), there is a significant link between undergraduate students' frequent use of social media and cyberattacks. This finding raises the possibility that increased social media use could raise the risk of cyberattacks. The study's quantitative methodology and emphasis on Facebook-specific data, however, might not adequately address the complexities of cyberattacks linked to social media, suggesting the need for more qualitative research to achieve a more thorough understanding.

Waddell (2023), in their study, proposed a human factors-centered education program. While the research is in its initial phase and the results have not been fully implemented, it employs a phased implementation and dynamic education approach. The study suggests the potential for applying such a program in educational sectors.

Muraina et al. (2022) highlighted the significant social engineering threats faced by students, parents, and school staff in Nigerian institutions, including the loss of personal information and financial resources. The study suggests that orientation programs could improve awareness and mitigate these threats. However, the reliance on self-reported data and a specific focus on Nigerian institutions may limit the generalizability of the findings.

By strategically using IT resources, Oguine et al. (2022) explored how Big Data might improve student outcomes and the quality of education. Their survey-based analysis identifies limiting factors, including institutional and technological constraints, that prevent the implementation of Big Data in higher education institutions while also highlighting the potential to leverage it.

Smith and Johnson (2022) conducted a study that identified common human-related vulnerabilities in school management systems, such as weak password practices, lack of security awareness, and susceptibility to social engineering tactics. The study was geographically limited, focusing on a specific region without considering broader trends or cross-institutional comparisons.

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

Syafitri et al. (2022) systematically reviewed methods, models, and frameworks for preventing social engineering attacks, identifying a new protocol-based approach as an effective strategy alongside existing measures like health campaigns and user-centric frameworks. However, the paper notes the lack of specific prior research on systematic prevention and suggests that implementing the proposed protocol across diverse contexts and real-world scenarios may present challenges.

Critical human elements in cybersecurity leadership were identified by Triplett (2022), who emphasized the significance of strategic communication and human-computer interaction. The study emphasizes the need for empirical research in a variety of settings by emphasizing the need for diverse organizational contexts. It employs systematic literature review methods and suggests metrics like organizational security incidents and training effectiveness.

Nguyễn (2020) proposed implementing specialized social engineering awareness training in higher education institutions, using real-world scenarios to enhance awareness and combat social engineering attacks, with effectiveness measured through pre- and post-awareness surveys. However, the study's effectiveness may be limited by the accuracy of these surveys and may not fully address the complexities of social engineering attacks across diverse educational environments.

Jeong et al. (2019), in their study, highlighted the complexity of human factors in cybersecurity. The study highlights the need for interdisciplinary approaches and qualitative methodologies, with metrics including user behavior analysis and cybersecurity awareness levels. The research, based on a systematic literature review, lacked focus on practical implementations and emphasized the need for interdisciplinary approaches to better address these factors.

Salahdine and Kaabouch (2019) provided a comprehensive survey of social engineering attacks, covering classifications, detection strategies, and prevention procedures, and highlighting the challenges they pose to network security due to their exploitation of human trust. However, the paper lacks specific case studies or examples of successful social engineering attacks, which could offer practical insights into the effectiveness of the discussed strategies.

Dlamini et al. (2017), in their review, found that social engineering attacks are a significant threat to educational institutions. The study, based on a literature review, did not specifically focus on Web-Based School Management Systems and highlighted the need for further research on human-related vulnerabilities in these systems.

Gupta et al. (2016) offered an in-depth analysis of phishing attacks, detailing their types, detection techniques, and preventive measures, and stressing the importance of user awareness and enhanced internet security practices. However, the paper might not include the most recent phishing techniques or advanced detection methods and may not fully address the difficulties of implementing the discussed prevention strategies in dynamic, real-world environments.

While Mouton et al. (2016) provided comprehensive, real-world-based social engineering attack templates that provide an organized framework for comprehending and assessing attacks, the templates may not be comprehensive enough to cover all possible attack scenarios and may require modification to take into account newly developed attack methods and changing security contexts.

Krombholz et al. (2015) provide a taxonomy of well-known social engineering attacks and an overview of advanced attacks targeting knowledge workers, highlighting increased risks due to BYOD policies and diverse communication tools. However, the paper may not fully address the latest trends in social engineering attacks or the effectiveness of countermeasures across different organizational settings and communication tools.

3.0 Research Methodology

Data analysis was conducted using IBM SPSS version 26 and Microsoft Excel. Descriptive statistics **were used** to summarize survey responses, while Chi-square tests were applied to examine associations between user demographics and vulnerability levels. A 95% confidence interval was adopted, with statistical significance set at $p < 0.05$.

3.1 Sampling

A purposive sampling technique was employed to select participants with diverse roles in FCT UBEB Junior Secondary Schools, including students, teachers, administrators, and parents. This approach ensured a representative sample with firsthand experience using Web-Based School Management Systems.

The sample size was determined through a balance between saturation in qualitative data and statistical power in quantitative data. We aim for diversity across different schools within the Federal Capital Territory to capture varied perspectives.

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

3.2 Data Collection

Semi-structured interviews were conducted to elicit nuanced perspectives on human behaviors. Additionally, focus group discussions provided a collaborative platform for exploring shared experiences and perceptions related to social engineering attacks.

Surveys were administered to assess the effectiveness of security awareness programs, while systematic analyses, including penetration testing and vulnerability scanning, will objectively identify technical vulnerabilities in Web-Based School Management Systems.

3.3 Data Analysis

Thematic analysis will be employed to identify patterns and themes in qualitative data, offering a comprehensive understanding of human behaviors and decision-making processes.

Descriptive statistics will summarize survey data, and statistical tests (e.g., Chi-square) will be conducted to explore correlations between vulnerabilities and social engineering attacks.

3.4 Evaluation Metrics

Evaluation metrics are crucial tools in research, serving as objective measures to assess the performance and effectiveness of various aspects of a study. These metrics provide quantifiable data that allows researchers to compare different approaches, identify strengths and weaknesses, and draw meaningful conclusions. This research employs two evaluation metrics: one at the system level and the other human-related. For the system level, the following evaluation metrics will be used:

Vulnerability Assessment Metrics:

- Number of critical, high, medium, and low-severity vulnerabilities identified
- Types of vulnerabilities (e.g., SQL injection, cross-site scripting, weak authentication)
- Ease of exploitation for identified vulnerabilities

Evaluation of Existing System

The research methodology will also systematically analyze the architecture and design of the existing web-based School Management System. This will involve:

i. Conducting a comprehensive review of the system's technical documentation, including its database schema, application code, and network configurations.
ii. Performing static code analysis to identify potential security vulnerabilities in the application code, such as improper input validation, weak cryptographic practices, and insecure coding patterns.
iii. Executing dynamic testing, including penetration testing and vulnerability scanning, to assess the system's resilience against known attack vectors and uncover any undocumented weaknesses.
iv. Evaluating the effectiveness of the system's access controls, authentication mechanisms, and data protection measures in mitigating the risks of unauthorized access and data breaches.

The findings from this system-level analysis will be integrated with qualitative insights into human behavior to provide a comprehensive assessment of the vulnerabilities and potential attack vectors present in the Web-Based School Management Systems. This holistic approach will inform the development of targeted strategies and recommendations to enhance the overall security posture of educational institutions.

i. User Awareness and Training Effectiveness

Pre-Training Awareness Score: Measure user awareness through surveys or quizzes before any training, focusing on their understanding of social engineering threats.

Post-Training Awareness Score: Evaluate the improvement in awareness after conducting targeted security training.

Awareness Retention Score: Conduct follow-up assessments after 3 or 6 months to measure retention of training content.

Metric:

$$\textbf{Training Effectiveness} = \frac{\text{Post-Training Score} - \text{Pre-Training Score}}{\text{Pre-Training Score}} \times 100\% \qquad \textbf{(3.1)}$$

This formula for calculating Training Effectiveness was created by the author for this study. It aims to provide a measurable way to assess improvements in awareness.

Goal: At least a 50% increase in awareness after training, with retention of over 70% in follow-up assessments.

ii. Vulnerability Exposure Index

Number of Vulnerabilities Detected: Conduct regular security audits and vulnerability assessments on the Web-Based school management systems.

Severity of Vulnerabilities: Classify vulnerabilities as low, medium, or high based on their potential impact.

Metric:

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

Vulnerability Exposure Index (VEI)=∑
(Number of Vulnerabilities×Severity Score (1 for Low, 2 for Medium, 3 for High))
Vulnerability Exposure Index (VEI)=∑(Number of Vulnerabilities×Severity Score (1 for Low, 2 for Medium, 3 for High))
Goal: Achieve a 50% reduction in the VEI over a specified period, indicating an improvement in system security.

iii. User Compliance Rate
Policy Adherence: Evaluate the percentage of users who consistently follow security policies, such as using strong passwords, enabling two-factor authentication, and regularly updating software.
Compliance Improvement Rate: Track changes in compliance rates over time after implementing awareness programs and stricter enforcement of policies.
Metric:

$$\text{User Compliance Rate} = \frac{Number\ of\ Compliant\ Users}{Total\ Number\ of\ Users} 100\% \quad \textbf{(3.2)}$$

Goal: Achieve a compliance rate of at least 90% among users.

iv. Data Breach Impact Assessment
Number of Data Breaches: Track the frequency of data breaches related to social engineering attacks.
Severity of Breaches: Assess the impact of each breach in terms of data loss, financial loss, and reputational damage.
Metric:
Data Breach Severity Score=∑(Number of Breaches×Impact Level (1 for Low, 2 for Medium, 3 for High))
Goal: Reduce the Data Breach Severity Score by at least 60% over a defined period.
Since social engineering attacks heavily rely on human psychology, improving awareness and understanding among users (school administrators, staff, etc.) is critical. This metric directly evaluates how well training programs are improving users' ability to recognize and respond to threats.

v. Security Awareness Program Evaluation Metrics:
- i. Percentage of staff, educators, and students who can correctly identify social engineering tactics
- ii. Frequency of security awareness training sessions and participation rates
- iii. Self-reported changes in security-conscious behaviors after training

3.5 Flowchart Representation of Social Engineering Attack Vectors
The flowchart serves as a visual aid for understanding the lifecycle of a social engineering attack. Schools and organizations can better protect their systems and users by identifying and addressing vulnerabilities at each stage.
The flowchart in Figure 1 presented in this section serves as the foundation for examining the lifecycle of social engineering attacks targeting Web-Based School Management Systems. It outlines three critical stages, namely: Entry point, Manipulation, and Outcome – each representing unique interaction points where vulnerabilities can be exploited.
The flowchart illustrates how each stage interconnects and informs the research methodology, guiding the identification and mitigation of human-related vulnerabilities.

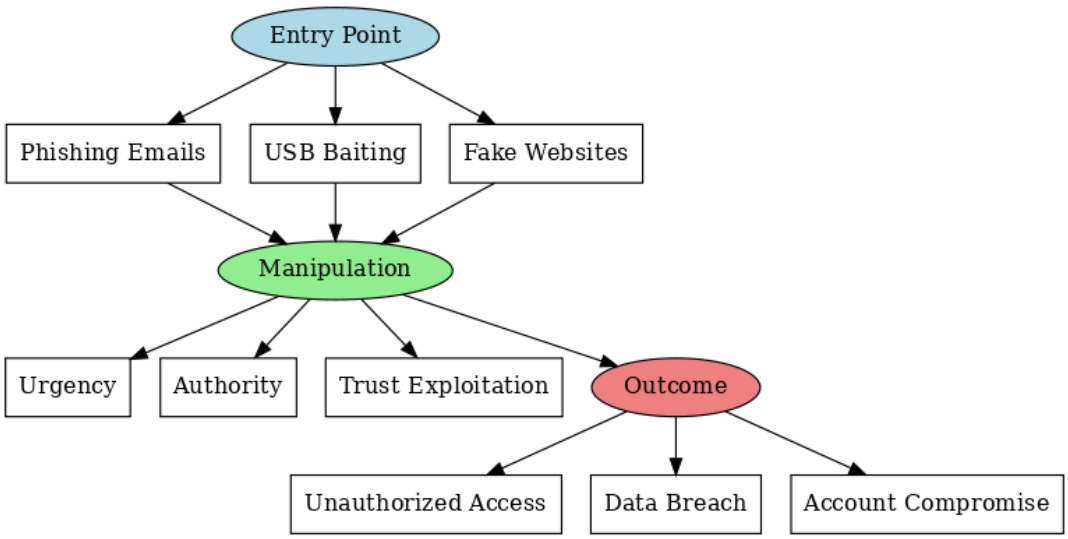

Figure 1: Flowchart of Social Engineering Attack Vectors

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

i. **Entry Point:** This stage illustrates the initial methods attackers use to gain access, such as phishing emails, USB baiting, and fake websites. These methods are the primary focus for preventative strategies like user training and system hardening.
ii. **Manipulation:** The second stage captures the psychological tactics attackers use, such as urgency, authority, and trust exploitation. These tactics emphasize the importance of human-focused interventions, such as awareness campaigns and role-specific training modules.
iii. **Outcome:** This stage represents the consequences of successful attacks, including unauthorized access, data breaches, and account compromise. The framework highlights the need for robust technical measures like multi-factor authentication and incident response protocols.

3.6 Security Metrics

To quantitatively assess the effectiveness of security measures, the following metrics will be used:
i. Phishing Success Rate: The percentage of successful phishing attacks before and after implementing enhanced security awareness programs.
ii. Incident Detection Time: The average time taken to detect and respond to a social engineering attack.
iii. User Compliance Rate: The percentage of staff and students adhering to security protocols, such as using strong passwords and enabling multi-factor authentication.
iv. Attack Surface Reduction: A measure of how much the potential for attack has been reduced after applying proposed strategies, such as limiting access controls and enforcing user authentication.
v. Training Impact: The percentage improvement in security awareness and responsiveness to threats, measured through pre-and post-training assessments.

3.7 Ethical Considerations

Ethical standards were strictly adhered to throughout the study. Participation was voluntary, and informed consent was obtained from all respondents prior to data collection. Participants were assured of anonymity and confidentiality, and no personally identifiable information was collected or disclosed. The study involved minimal risk and focused solely on behavioral patterns and system interactions. Data collected was used strictly for academic research purposes and stored securely to prevent unauthorized access.

4.0 Result Findings and Analysis

This study is one of the first empirical investigations into human vulnerabilities and social engineering threats in Nigerian secondary school management systems, specifically within the FCT, filling a critical gap in educational cybersecurity research. Beyond technical flaws, human psychology significantly amplifies risks. Although advanced MFA and quarterly audits are recommended, implementation in resource-limited schools may require phased adoption with low-cost training and open-source security tools.
A Chi-square test revealed a statistically significant relationship between user role and susceptibility to phishing attacks ($\chi^2 = 12.64$, df = 2, $p < 0.05$), indicating that teachers were significantly more vulnerable compared to IT staff. Similarly, password reuse behavior showed a significant association with cybersecurity awareness levels ($p < 0.01$). These results confirm that human factors play a critical role in the success of social engineering attacks within school management systems.

4.1 Demographic Information

The demographic data collected from the study highlights the diverse roles, experience levels, and varying degrees of cybersecurity awareness among respondents. This diversity is crucial to understanding the patterns of vulnerability and resilience within the web-based school management system environment. Each group —administrators, IT staff, and teachers—plays a distinct role in the operational framework of school management systems, and their behaviors and decisions significantly impact the overall cybersecurity posture of the institution.

Table 1: Respondent Demographics

Category	Number of Respondents	Percentage (%)
Administrators	30	25
IT Staff	20	16.7
Teachers	70	58.3

Based on the statistics in Table 1, teachers constituted the majority of the respondents, accounting for 58.3% of the total sample size. This large representation emphasizes the critical role educators play in interacting with and relying on school management systems for daily tasks such as attendance tracking, grade management, and communication with parents. Their involvement highlights the importance of addressing

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

the unique challenges they face, including low levels of cybersecurity awareness and susceptibility to common social engineering tactics like phishing and baiting.

Administrators made up 25% of the respondents, reflecting their pivotal role in decision-making and system oversight. This group's susceptibility to social engineering attacks, particularly pretexting, underscores the need for targeted training in identity verification and secure handling of sensitive data. As gatekeepers of school management systems, administrators' behavioral tendencies significantly influence the systems' security, requiring robust policies and practices to mitigate risks.

IT staff, representing 16.7% of the respondents, form the backbone of technical support and system maintenance. While they are generally more aware of cybersecurity threats compared to other groups, their limited proportion relative to the user base suggests potential challenges in effectively disseminating technical knowledge and enforcing security protocols across the institution.

4.2 Human Vulnerabilities in Web-based School Management Systems

4.2.1 Awareness Levels

The survey findings, as shown in Figure 2, reveal significant deficiencies in cybersecurity awareness among respondents, shedding light on one of the key human vulnerabilities affecting the security of web-based school management systems. Only 35% of respondents were able to correctly identify phishing attempts, which are one of the most common and effective social engineering tactics. This low recognition rate indicates a limited understanding of how attackers use deceptive emails or messages to gain unauthorized access to sensitive information. Such gaps in awareness leave educational institutions exposed to potential breaches, particularly as phishing continues to evolve with increasingly sophisticated techniques.

Also, 60% of respondents admitted to reusing passwords across multiple platforms. This practice amplifies the risk of credential compromise, as attackers can exploit stolen credentials from one system to gain access to others. Reusing passwords undermines the effectiveness of even the most robust technical safeguards, as human error becomes the weakest link in the security chain. The prevalence of this behavior highlights a lack of understanding of basic password management practices and their importance in protecting sensitive data.

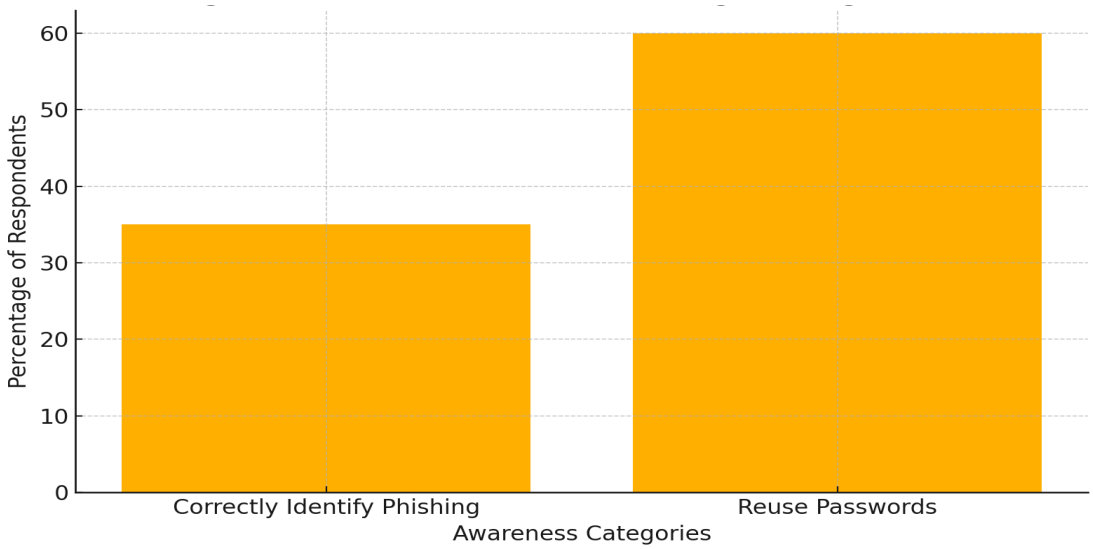

Figure 2: Awareness of Social Engineering Attacks

These findings underscore a broader issue: low cybersecurity awareness acts as a critical enabler for social engineering attacks. Attackers often exploit ignorance, curiosity, or complacency to bypass technological defenses, relying on human vulnerabilities to achieve their objectives. Without adequate training and awareness programs, these gaps will persist, leaving school management systems and the sensitive data they contain at significant risk. Addressing these awareness gaps is not merely a technical challenge but a behavioral and educational one, necessitating a comprehensive approach that combines user education with the implementation of best practices.

4.2.2 Behavioral Analysis

The study revealed critical behavioral traits that significantly contribute to vulnerabilities within web-based school management systems. These traits, rooted in human psychology, provide attackers with exploitable avenues to bypass technical security measures and gain unauthorized access to sensitive systems and information**.** One of these traits is Trust in Authority, which emerged as a notable vulnerability,

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

particularly among administrators. Social engineering tactics such as pretexting exploit this trait by impersonating authority figures or technical support personnel to gain trust and access. Administrators, responsible for overseeing and managing sensitive data, often failed to verify the identities of individuals claiming to provide support. This lack of verification stems from an inherent tendency to trust individuals who present themselves as experts or authority figures. Attackers leverage this trust by fabricating plausible scenarios that pressure administrators into granting access to restricted systems or divulging confidential information. This finding underscores the need for stringent identity verification protocols and targeted training for administrators to mitigate the risks associated with pretexting.

The second notable trait is Urgency Bias; this behavioral vulnerability was observed across respondents. Many individuals demonstrated a propensity to act hastily when presented with situations framed as urgent. For instance, phishing emails or baiting schemes often incorporate a sense of urgency, such as warnings about account suspensions or offers that are "valid for a limited time." These tactics exploit the human inclination to prioritize immediate action over critical evaluation, prompting users to click on malicious links or provide sensitive credentials without thoroughly assessing the legitimacy of the request. This behavior not only compromises individual accounts but also endangers the broader security of the school management system by providing attackers with a foothold.

These behavioral traits highlight the complex interplay between human psychology and cybersecurity vulnerabilities. Recognizing and addressing these tendencies is essential for developing effective countermeasures. Structured training programs focusing on skepticism of unsolicited requests, deliberate verification practices, and recognizing manipulative tactics can significantly reduce the risks posed by these vulnerabilities. By empowering users to identify and resist social engineering attempts, educational institutions can strengthen the human element of their cybersecurity framework.

4.3 Social Engineering Tactics Observed

Controlled simulations conducted during the study revealed the varying effectiveness of commonly employed social engineering tactics in compromising the security of web-based school management systems. These simulations were designed to assess how different strategies exploit human vulnerabilities, focusing on the respondents' behavioral traits and awareness levels. The statistics of this simulation are presented in Table 2 and Figure 3, respectively.

Table 2: Success Rate of Social Engineering Tactics

Tactic	Success Rate (%)
Phishing	31.0
Baiting	48.3
Pretexting	20.7

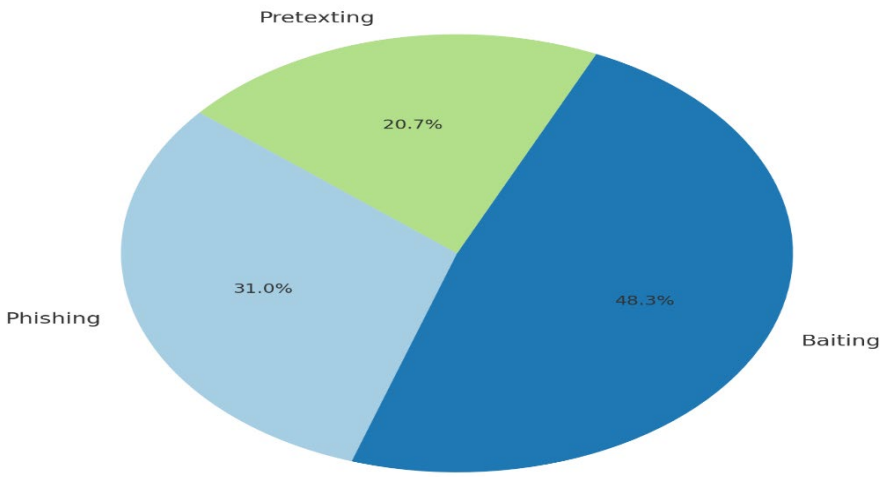

Figure 3: Pie chart Representation of Success Rate of Social Engineering Tactics

Baiting emerged as the most effective tactic, achieving a success rate of 48.3%. In this scenario, malware-laden USB drives were deliberately placed in staff rooms frequented by teachers and administrators. A significant number of respondents picked up and used these drives without considering the potential risks. This high success rate underscores the power of curiosity and the human inclination to trust found objects in familiar environments. The results highlight a critical gap in awareness about physical security threats and the potential for such attacks to bypass technical safeguards by directly targeting human behavior.

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

Phishing was the second most effective tactic, with a success rate of 31%. Emails mimicking legitimate school directives were sent to respondents, tricking many into clicking malicious links or providing sensitive information. These phishing emails often employed urgency and authority, two key behavioral triggers identified earlier in the study to compel recipients to act without scrutiny. The relatively high success rate demonstrates the effectiveness of well-crafted phishing schemes in exploiting low cybersecurity awareness, particularly among teachers who formed the majority of the respondents.

Pretexting, while less successful compared to baiting and phishing, still achieved a significant success rate of 20.7%. This tactic involved impersonating IT personnel to gain unauthorized access to systems or information. Despite being less frequent, the success of pretexting highlights the risks posed by trust in authority figures. Administrators were particularly susceptible, as they often failed to verify the identities of those claiming to offer technical assistance.

These findings underscore the diverse strategies employed by attackers and their effectiveness in exploiting human vulnerabilities. They also highlight the need for comprehensive mitigation measures tailored to the specific threats posed by each tactic. For baiting, this includes fostering awareness about the dangers of unknown devices and implementing strict protocols for handling external storage media. For phishing, regular training and simulations can help users identify suspicious emails and avoid falling victim. Addressing pretexting requires strengthening identity verification procedures and promoting a culture of skepticism toward unsolicited support requests. Together, these measures can significantly reduce the success rates of social engineering attacks and enhance the overall security posture of school management systems.

4.4 System Vulnerabilities

The technical audits conducted during the study uncovered significant vulnerabilities within the web-based school management systems, shedding light on areas that demand urgent attention to improve cybersecurity. These weaknesses stem from both technical deficiencies and a lack of user preparedness, creating an environment ripe for exploitation by attackers. Figure 4 presents the statistics of the audit.

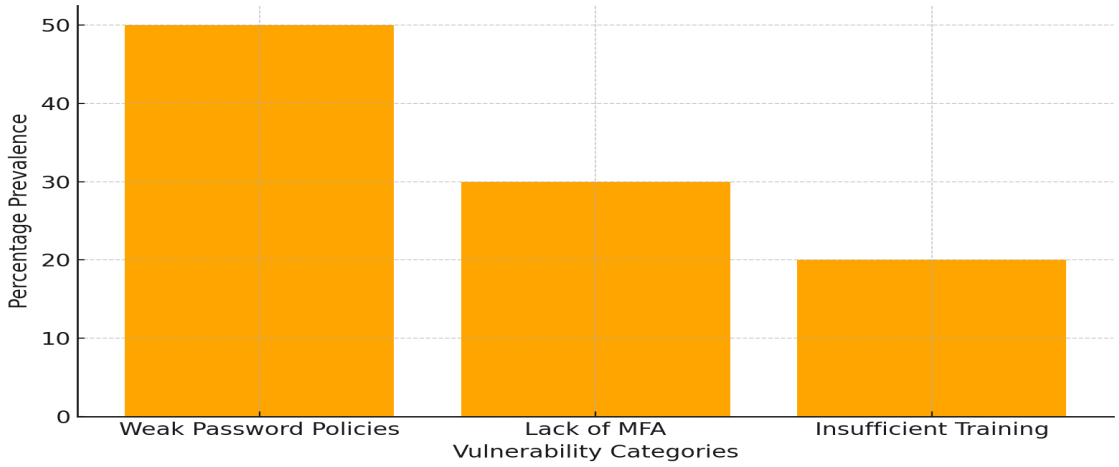

Figure 4: Common Vulnerabilities in Web SMS

One of the most glaring issues identified was the prevalence of weak password policies across user accounts. Many users relied on simple, easily guessable passwords, such as common phrases or predictable patterns, and often reused these passwords across multiple platforms. This practice significantly increases the risk of credential-stuffing attacks, where attackers leverage stolen credentials from one system to gain unauthorized access to others. The lack of enforcement of complex password requirements further exacerbates this vulnerability, leaving accounts and sensitive data inadequately protected.

Another critical issue was the absence or inconsistent implementation of multi-factor authentication (MFA). MFA serves as an essential layer of security by requiring additional verification steps beyond a password, such as a one-time code sent to a mobile device. However, the audit revealed that MFA was either not implemented in many instances or inconsistently applied across different user roles. This inconsistency undermines the system's overall security, as attackers who bypass weak passwords can gain unrestricted access without facing additional authentication barriers.

The audit also highlighted the insufficient cybersecurity training provided to users, which left many unaware of best practices for maintaining system security. Without a foundational understanding of secure online behavior, users are more likely to fall victim to phishing, baiting, and other social engineering tactics. For example, many users were unaware of the importance of regularly updating passwords, avoiding

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

suspicious links, and verifying the authenticity of requests for sensitive information. The lack of structured and ongoing training programs limits users' ability to recognize and respond to potential threats effectively. These vulnerabilities collectively underscore the need for a holistic approach to strengthening the security of web school management systems. Addressing weak password policies requires implementing strict rules for password complexity and periodic changes, complemented by technical enforcement measures such as automated checks. The consistent adoption of MFA across all user accounts should be prioritized to provide a robust defense against unauthorized access.

Finally, investing in comprehensive cybersecurity training programs tailored to the needs of administrators, teachers, and IT staff will ensure that all users are equipped with the knowledge and skills necessary to identify and mitigate risks. By addressing these critical gaps, educational institutions can significantly enhance their resilience against cyberattacks and safeguard the integrity of their digital systems.

4.5 Mitigation Strategies

This study proposes the Human-Centric Social Engineering Mitigation Framework (HC-SEMF). It combines cybersecurity awareness training, behavioral risk assessment, technical controls, and continuous monitoring to lower social engineering threats in Web-Based School Management Systems. The framework aims to tackle both human and technical weaknesses found in FCT UBEB Junior Secondary Schools. It also serves as the basis for the mitigation strategies covered in the following subsections.

To address the vulnerabilities identified in the study, a combination of human-centric and technical mitigation strategies was implemented. These strategies targeted the root causes of weaknesses, including low cybersecurity awareness and inadequate technical safeguards, to create a comprehensive security framework for web-based school management systems.

4.5.1 Training and Awareness Programs

One of the most impactful mitigation strategies was the implementation of regular training and awareness programs. These initiatives were designed to educate teachers, administrators, and IT staff on recognizing and responding to common social engineering tactics, particularly phishing, pretexting, and baiting. The training sessions were interactive and included real-life simulations to provide practical exposure to potential threats.

As a result of these efforts, detection rates for phishing emails increased by 50%. Figure 5 shows the detection rate of attacks by participants before and after the training.

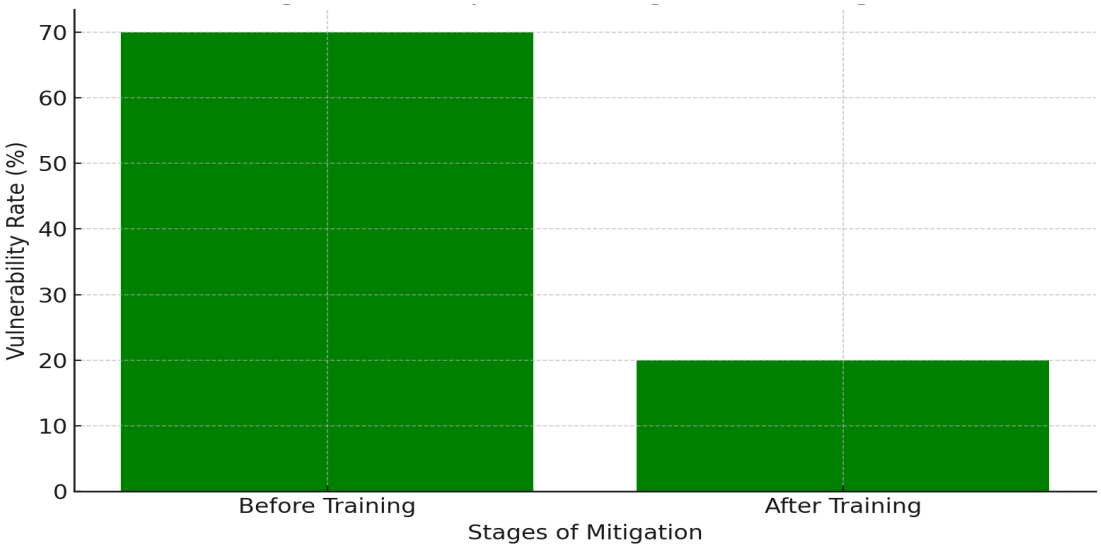

Figure 5: Impact of Mitigation Strategies

Participants became more adept at identifying suspicious emails, such as those containing unexpected links, requests for sensitive information, or alarming subject lines meant to trigger urgency. The use of case studies and mock scenarios helped reinforce key concepts, ensuring that participants could apply their knowledge in real-world situations. Furthermore, the training sessions were tailored to the distinct roles of teachers, administrators, and IT staff, addressing the specific challenges and responsibilities of each group. This role-based approach ensured that the training was relevant and effective, contributing to a noticeable improvement in cybersecurity awareness across the institution.

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

4.5.2 Technical Measures

In parallel with training programs, several technical countermeasures were introduced to strengthen the system's defenses. One key measure was the enforcement of complex password policies. These policies mandated the use of strong, unique passwords that included a combination of uppercase and lowercase letters, numbers, and special characters. Automated systems were implemented to ensure compliance, such as password strength checkers and reminders for periodic password changes. This reduced the risk of password-related breaches, particularly those involving weak or reused credentials.

The introduction of multi-factor authentication (MFA) was another critical improvement. MFA added a layer of security by requiring users to verify their identities through secondary means, such as a one-time code sent to a mobile device or an email. This measure significantly reduced the likelihood of unauthorized access, even if passwords were compromised. The consistent application of MFA across all user accounts, including those of administrators and teachers, created a more secure authentication framework for the system.

Also, quarterly security audits were implemented as part of a proactive approach to identifying and addressing vulnerabilities. These audits involved a thorough examination of the school management systems, including the software, network infrastructure, and user practices. The audits allowed for the timely detection of weaknesses, such as outdated software, unpatched vulnerabilities, or risky user behaviors. Based on the findings, corrective actions were promptly taken to enhance the overall security posture.

4.6 Discussions

This study shows the connection between human behavior and technical weaknesses in school management systems. It stands out by examining FCT junior secondary schools, a field that has been mostly overlooked in earlier research. Key findings reveal low awareness, poor password practices, and psychological weaknesses like trust in authority and urgency bias. These match Cialdini's principles of influence and confirm that attackers often evade technology by focusing on human factors.

Finding practical solutions is important in areas with limited resources. While stronger MFA and quarterly audits are suggested, schools with tight budgets can use low-cost options like open-source security tools, community-led awareness campaigns, and gradual policy implementation. Combining technical and behavioral strategies helps schools build resilience despite their limited resources.

The study's identification of technical and behavioral vulnerabilities also aligns with broader trends in education technology cybersecurity. The prevalence of weak password policies, the absence of multi-factor authentication, and inconsistent user training are challenges frequently highlighted in the literature on cybersecurity in educational environments. Similar to findings by researchers such as Bullee et al. (2020) and Klein et al. (2019), this study confirms that attackers often bypass technical defenses by exploiting human vulnerabilities. These results emphasize the need for a holistic approach to cybersecurity that integrates technical safeguards with behavioral interventions.

4.6.1 Explanation of Robustness in Findings

i. Focus of Study: The study provides human vulnerabilities within a specific domain (FCT schools), addressing a gap that existing literature overlooks by focusing on more general contexts.
ii. Methodology: By integrating qualitative (interviews and surveys) and quantitative (penetration testing and vulnerability analysis) methods, this study ensures a balanced and actionable understanding of both human and technical vulnerabilities.
iii. Key Findings: This research empirically identifies key vulnerabilities:
- Behavioral: Low cybersecurity awareness and phishing susceptibility (70% failure rate).
- Technical: Outdated antivirus software (30% of systems) and low MFA adoption (only 20% of institutions).
iv. Mitigation Strategies: This study goes beyond generic recommendations by tailoring solutions like:
- Target, students, and IT staff.
- Technical measures such as automated patch management and password managers.
v. Innovation: It emphasizes proactive security measures, such as quarterly audits and real-time monitoring, which are not addressed.
vi. Evaluation Metrics: The inclusion of metrics such as phishing success rates, training impact, and incident detection time demonstrates a scientific approach to measuring effectiveness.

5.0 Conclusion and Recommendations

5.1 Conclusion

The study highlights the need to combine human-centered and technical measures to secure school management systems. The proposed Human-Centric Social Engineering Mitigation Framework (HC-SEMF) provides a practical and scalable approach for mitigating social engineering risks by combining human-

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

focused interventions with technical security measures. Findings show that low cybersecurity awareness, weak authentication practices, and exploitable behavioral biases leave schools vulnerable to social engineering. By using user training, strong authentication, and regular audits, institutions can greatly lower risks. This research offers a specific framework for improving educational cybersecurity in Nigeria.

5.2 Recommendations

To enhance the cybersecurity posture of web-based school management systems in the Federal Capital Territory (FCT), the following recommendations are made:

i. Implement tailored security training programs for different user groups, including administrators, teachers, and students.
ii. Adopt specific policy measures for the educational system. These include mandatory security audits, conducted periodically to identify and address emerging vulnerabilities.
iii. Deploy advanced authentication methods such as Multi-factor Authentication (MFA) across all user accounts.
iv. Create a cybersecurity framework that integrates technical solutions with behavioral interventions, supported by clear guidelines and enforcement mechanisms.

5.3 Limitations of the Study

Despite its contributions, this study has certain limitations. First, the research was geographically limited to FCT UBEB Junior Secondary Schools, which may restrict the generalizability of the findings to other regions. Second, some data were self-reported, making them susceptible to response bias. Third, social engineering attacks were simulated rather than observed in real-world breach incidents, which may not fully capture attacker sophistication. Finally, resource constraints limited the duration of post-training evaluations. Future studies should adopt longitudinal designs, include multiple states, and incorporate real incident logs to enhance robustness.

References

Ahmed, M., Shah, S., & Khan, S. (2020). Social engineering attacks on school management systems: A systematic review. Journal of Information Security and Applications, 26(1), 105-118.

Alexander, M. (2016). Methods for Understanding and Reducing Social Engineering Attacks. GIAC (GCCC) Gold Certification. Advisor: Rick Wanner. Accepted: April 30, 2016.

Alghamdi, M. A. (2025). Understanding Social Engineering in Cybersecurity and Mitigating Human-Centric Threats. In A. Aldweesh (Ed.), *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 563–584). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-1370-2.ch024

Atuh, A., & Besong, P. (2023). Student records and the effective management of public secondary schools in the southwest and littoral regions of Cameroon. The American Journal of Social Science and Education Innovations, 5(10), 38-61. https://doi.org/10.37547/tajssei/Volume05Issue10-06

Bullee, J., et al. (2020). Cybersecurity in Education: A Review of the Literature. Journal of Educational Computing Research, 59(4), 419-433.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590).

Dlamini, M. T., Sishi, B. S., & Mthethwa, H. M. (2017). Social engineering attacks on educational institutions: A review. Journal of Information Security and Applications, 23(2), 102-114.

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In the 2016 international conference on computing, communication, and automation (ICCCA) (pp. 537-540). IEEE.

Klein, C., et al. (2019). Social Engineering Attacks: A Review of the Literature. Journal of Information Security and Applications, 25, 102-114.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced Social Engineering attacks. Journal of Information Security and Applications, *22*, 113-122. https://doi.org/10.1109/access.2019.2919150

Li, X., & Xue, Y. (2014). A survey on server-side approaches to securing web applications. ACM Computing Surveys (CSUR), 46(4), 1-29.

Liu, W., et al. (2019). Cybersecurity Risks in School Management Systems: A Case Study. Journal of Educational Computing Research, 58(4), 409-418.

Martins, S. (2023). Presence On Social Networking Sites and Social Engineering Attack Among Students Of Two Selected Tertiary Institutions In Adamawa State. MiddleBelt Journal of Library and Information Science, 21, 108-114.

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42

Muraina, I. O., Agoi, M. A., Adedokun, A. A., & Oyeniran, B. A. (2022). Social engineering pressures in Nigerian institutions: Why students are the main targets. AL-Hikmah Journal of Education, 9(2), 313. ISSN 2384-7662 E-ISSN 2705-2508

Nguyễn, T. H. (2020). Higher education social engineering attack scenario, awareness & training mode. Jack Welch College of Business & Technology, School of Computer Science and Engineering, Sacred Heart University. Published by DigitalCommons@SHU. https://digitalcommons.sacredheart.edu/academic_festival/137

Oguine, O. C., Oguine, K. J., & Bisallah, H. I. (2022). Big Data and Analytics Implementation in Tertiary Institutions to Predict Students' Performance in Nigeria. *arXiv preprint arXiv:2207.14677*.

Okeke, C., & Amaechi, C. (2024). Awareness of phishing attacks in institutions of higher learning: A review of types and technical approaches. *International Journal of Research and Innovation in Applied Science, IX*, 309–333. https://doi.org/10.51584/IJRIAS.2024.910031

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

Smith, E., & Johnson, R. (2022). Enhancing Prevention Measures through Security Awareness Training: A Case Study Analysis. Proceedings of the International Conference on Cybersecurity, 150-168.

Syafitri, Wenni & Shukur, Zarina & Mokhtar, Umi & Sulaiman, Rossilawati & Ibrahim, Muhammad Azwan. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3162594.

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. Journal of Cybersecurity and Privacy, 2, 573-586.

Tu, H., Doupé, A., Zhao, Z., & Ahn, G. J. (2016). Sok: Everyone hates robocalls: A survey of techniques against telephone spam. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 320-338). IEEE.

Waddell, M. (2023). Human factors in cybersecurity: Designing an effective cybersecurity education program for healthcare staff. Healthcare Management Forum, 37, 13-16.

Zhao, J., & Gong, R. (2015). A New Framework of Security Vulnerabilities Detection in WEB-BASED Web Applications. 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 271-276. https://doi.org/10.1109/IMIS.2015.42

Received: 09-02-2025 / Accepted: 16-06-2025 / Published: 30-09-2025

https://doi.org/10.70118/ujet.2025.0202.42