September 30, 2025 Vol. 9 No. 9 E-ISSN 3027-0952 P-ISSN 3027-2033
International Journal of
CONVERGENT AND INFORMATICS SCIENCE RESEARCH (IJCISR)
www.harvardpublications.com

STRENGTHENING CYBERSECURITY AWARENESS THROUGH PHISHING SIMULATIONS: EVIDENCE FROM TERTIARY INSTITUTIONS IN TARABA STATE, NIGERIA

***AUGUSTINE NDUDI EGERE[1], HUSSEINI USMAN YARO[2]; & AARON IHE NWOKOCHA[3]**
Department of Computer Science, Federal Polytechnic Bali[1,,3]. ICT Unit, Federal Polytechnic Bali, Taraba State, Nigeria[2]
Corresponding Author: austinendudi@yahoo.com
DOI: https://doi.org/10.70382/hijcisr.v09i9.048

Abstract

Phishing remains one of the most persistent cybersecurity threats to academic institutions, exploiting human vulnerabilities more than technological loopholes. This study evaluates the effectiveness of simulated phishing interventions in enhancing staff awareness across three tertiary institutions in Taraba State, Nigeria (codenamed UNI A, UNI B, and UNI C). With the cooperation and approval of each institution's ICT director, more than 900 phishing emails themed

Keywords:
Cybersecurity, Phishing Simulation, Staff Awareness, Higher Education, Nigeria

INTRODUCTION

Phishing remains one of the most persistent and effective cyberthreats facing organisations worldwide, relying primarily on social-engineering techniques that exploit human judgement rather than technical vulnerabilities (APWG, 2023; Morrow, 2024). Academic institutions are particularly attractive targets because they manage large volumes of sensitive personal, financial, and research data, operate complex IT ecosystems, and rely heavily on email communication conditions that increase both the likelihood and the impact of successful phishing campaigns (Borgman, 2018; Dolliver, Ghazi-Tehrani, & Poorman, 2021). Advances in artificial intelligence and automation have made phishing campaigns increasingly sophisticated and personalised, posing heightened risks to higher education institutions with limited cybersecurity resources (Nayak, Marino, & Camp, 2021; Bose &

around a "13-month salary bonus payment" were disseminated to staff, with several hundred responses recorded. A quasi-experimental design was employed, consisting of a pre-intervention survey, the phishing simulation, and a post-intervention survey. Results revealed high initial susceptibility, with a majority of respondents engaging with the phishing email. Post-intervention analysis demonstrated statistically significant improvements in staff self-assessed awareness and phishing detection skills, as confirmed by Chi-Square testing ($p < 0.001$). Institutional comparisons indicated variations in susceptibility and reporting culture, suggesting that contextual factors such as communication practices and ICT exposure influence vulnerability levels. The findings highlight the urgent need for continuous, customized awareness programs, formalized incident reporting mechanisms, and integration of phishing simulations into professional development policies within Nigerian higher education.

Leung, 2022). Research has consistently shown that phishing susceptibility is not confined to particular demographic or educational groups; even highly educated staff can be deceived by well-crafted emails (Li et al., 2020; Bach, Kamenjarska, & Žmuk, 2022). To mitigate this vulnerability, organisations increasingly adopt phishing simulations as both diagnostic and educational tools. These simulations allow institutions to measure staff susceptibility through click rates and reporting behaviours, while debriefing and awareness training reinforce detection skills (Beu et al., 2023; Jampen et al., 2020; Bichnigauri et al., 2024). Despite their widespread use in developed contexts, little is known about how institutional culture, ICT readiness, and communication practices influence susceptibility and response in under-researched higher education systems, particularly in sub-Saharan Africa.

This study addresses this gap by examining phishing susceptibility and awareness among staff in three tertiary institutions in Taraba State, Nigeria, anonymised as **UNI A, UNI B,** and **UNI C.** With approval and oversight from each institution's ICT director, a large-scale phishing simulation was conducted in which over 900 emails were disseminated, generating several hundred staff responses. The study employed a quasi-experimental design comprising a pre-intervention survey, a phishing simulation, and a post-intervention survey. The phishing email adopted a culturally salient financial theme a "13-month salary bonus" to reflect the type of incentive-based messaging often exploited by real attackers. The objectives of this study are to:

1. Assess baseline cybersecurity awareness among staff in UNI A, UNI B, and UNI C.
2. Measure staff engagement and reporting behaviours during the phishing simulation.
3. Evaluate changes in self-assessed phishing awareness and detection skills before and after the intervention.
4. Compare institutional differences in susceptibility and reporting culture, exploring contextual explanations.

By testing the hypothesis that a structured phishing simulation and awareness cycle significantly improves staff preparedness (Beu et al., 2023; Jampen et al., 2020), this study contributes to cybersecurity scholarship in three ways. Methodologically, it provides a model for ethically sound phishing simulations in resource-constrained higher education contexts. Practically, it offers actionable recommendations for embedding phishing awareness into institutional staff development programmes and incident-reporting systems. Conceptually, it enriches the literature on cybersecurity resilience in African higher education by showing how cultural and organisational factors shape susceptibility to social engineering.

Literature Review

The evolution of phishing reflects the increasing sophistication of cybercrime. Early phishing campaigns in the late 1990s and early 2000s often relied on crude email messages with obvious spelling errors or suspicious links, yet many users still succumbed to these attacks (Hong, 2012). Over time, phishing has advanced into highly personalised, targeted strategies known as spear-phishing, where attackers leverage publicly available information to craft convincing messages (Jampen, Gürses, & Čapkun, 2020). The Anti-Phishing Working Group (2023) reported nearly five million phishing attacks in 2023, the highest on record, with evidence that artificial intelligence and automation are increasingly being used to design context-aware phishing content. Bose and Leung (2022) argue that machine learning enables attackers to adapt their messaging to different user profiles, thereby reducing the effectiveness of traditional rule-based detection systems.

The growing adoption of artificial intelligence in phishing campaigns underscores the inadequacy of purely technical solutions. Nayak, Marino, and Camp (2021) contend that as phishing becomes more context-driven and adaptive, user-focused defences such as awareness training and behaviour modification become critical. This perspective aligns with the assertion by Hong (2012) that phishing is fundamentally a socio-technical problem, requiring strategies that combine technological safeguards with user education.

Psychological and Human Factors in Phishing Susceptibility

Understanding why individuals fall victim to phishing requires consideration of psychological and behavioural factors. According to Beu et al. (2023), individual susceptibility varies significantly depending on traits such as trust, curiosity, and risk perception. Their study found that employees motivated by curiosity were more likely to click on suspicious links, while those with higher institutional trust tended to comply with authority-laden phishing messages. Similarly, Jampen et al. (2020) argue that urgency cue, such as messages suggesting limited time to act, amplify susceptibility by encouraging impulsive decisions.

Other studies support this view. Yeng, Fauzi, Yang, and Nimbe (2022) reported that healthcare staff who fell victim to simulated phishing emails frequently cited urgency and trust in institutional communication as the main reasons for engagement. Li et al. (2020) add that demographic factors, such as age and job role, may also play a role, although

susceptibility is not limited to any one group. Interestingly, Bach, Kamenjarska, and Žmuk (2022) found that higher educational attainment does not necessarily protect against phishing; in their study, well-educated professionals sometimes exhibited higher click rates than less educated counterparts, suggesting that overconfidence may paradoxically increase vulnerability.

Together, these findings highlight the importance of simulations and training programmes that account for cognitive biases. Effective awareness interventions should not only provide technical knowledge but also address psychological factors such as trust in authority, financial incentives, and curiosity-driven behaviour.

Phishing in Higher Education Institutions

Higher education institutions are uniquely vulnerable to phishing due to the breadth of sensitive data they manage and their reliance on open communication systems. Borgman (2018) explains that universities often process "grey data" such as student grades, research outputs, and financial information, which, if stolen, can be monetised or exploited for identity theft. Dolliver, Ghazi-Tehrani, and Poorman (2021) note that universities may experience millions of attempted cyberattacks weekly, many of which involve phishing as the initial entry point.

Research further shows that staff and students are both susceptible to phishing. Goel, Williams, and Dincelli (2017) observed that approximately one-quarter of students clicked on phishing messages in a controlled study, with nearly half of them proceeding to interact with malicious content. Li et al. (2020) similarly found that at least 20% of university staff clicked on simulated phishing emails, indicating a persistent vulnerability even among ICT-literate populations. These findings underscore that higher education institutions cannot assume digital familiarity equates to cyber resilience.

The openness of academic environments also exacerbates risk. Singar and Akhilesh (2020) emphasise that universities are particularly attractive to cybercriminals because of their decentralised IT structures and diverse user groups, ranging from students and administrative staff to researchers. This complexity creates multiple entry points for attackers. Additionally, the culture of openness in academia often conflicts with rigid cybersecurity practices, further complicating institutional defences.

Phishing Simulation as a Tool for Awareness and Behaviour Change

Phishing simulations have emerged as an important mechanism for assessing and improving resilience. According to Jampen et al. (2020), controlled simulations allow institutions to test staff responses in realistic conditions while maintaining security. These exercises typically measure click-through rates, data submissions, and reporting behaviours, providing a snapshot of institutional readiness. Importantly, simulations also serve as educational tools, fostering experiential learning.

Beu et al. (2023) found that repeated phishing simulations, when combined with feedback, reduce click rates over time and promote incident reporting. Bichnigauri et al. (2024) argue that simulations are most effective when tailored to organisational contexts, reflecting the kinds of messages staff are most likely to receive. For example, simulations

themed around payroll, institutional communication, or funding opportunities are more likely to reveal real vulnerabilities than generic messages.

Case studies further demonstrate the utility of simulations. In healthcare, Yeng et al. (2022) observed that over 60% of staff clicked on phishing emails during initial simulations, but susceptibility declined after awareness activities, illustrating the importance of iterative training. In corporate settings, Jampen et al. (2020) similarly documented measurable improvements in staff detection skills following regular simulations and structured debriefing. These findings collectively suggest that simulations should not be viewed solely as diagnostic tools but as integral components of cybersecurity education.

Phishing in the African and Nigerian Context

While phishing has been extensively studied in Western and Asian contexts, African higher education institutions remain underrepresented in the literature. The African Union (2021) reports that cybercrime is growing rapidly across the continent, with phishing and social engineering representing the most common attack vectors. Nigerian universities, in particular, face rising risks as they undergo digital transformation without corresponding investment in cybersecurity infrastructure.

Few empirical studies directly examine phishing susceptibility in Nigerian higher education. Most existing research focuses on broader ICT adoption challenges, such as limited funding, inadequate staff training, and unreliable internet access (Singar & Akhilesh, 2020). These structural issues may indirectly increase vulnerability to phishing, as institutions often lack robust security awareness programmes. Anecdotal evidence suggests that phishing attacks exploiting financial incentives, payroll systems, and scholarship opportunities are particularly effective in Nigeria, but systematic studies remain scarce.

This gap underscores the need for context-specific research. As Beu et al. (2023) note, susceptibility to phishing is shaped not only by individual behaviour but also by institutional culture and resources. Studying Nigerian institutions provides an opportunity to understand how factors such as resource constraints, communication practices, and cultural attitudes toward authority influence susceptibility. Such insights are crucial for developing effective, locally adapted awareness strategies.

Theoretical framework

Phishing susceptibility has been widely examined through behavioural and socio-technical lenses, offering useful theoretical grounding for this study. Protection Motivation Theory (PMT) is especially relevant, as it explains how individuals assess threats and adopt coping strategies when confronted with potential risks. According to PMT, user behaviour is shaped by perceived severity, vulnerability, response efficacy, and self-efficacy (Rogers, 1975; Boss et al., 2015). In the context of phishing, staff who underestimate the severity or believe they are less vulnerable are more likely to engage with malicious links, while those with higher self-efficacy in identifying threats are less

susceptible. Complementing PMT, the Theory of Planned Behavior (TPB) offers insights into how attitudes, subjective norms, and perceived behavioural control shape responses to phishing attempts (Ajzen, 1991). Within higher education institutions, cultural and organisational norms strongly influence staff behavior, messages appearing to come from authority figures may override individual caution. Integrating PMT and TPB thus highlights the importance of both individual cognitive appraisals and institutional culture in shaping phishing susceptibility.

This theoretical framing situates the present study within a broader body of work on cybersecurity behaviour, enabling a richer interpretation of how Nigerian higher education staff respond to phishing attempts and why tailored interventions are necessary.

Conceptual Framework and Research Gap

The literature collectively demonstrates that phishing is a socio-technical challenge shaped by evolving attacker tactics, human psychological factors, and institutional contexts. In higher education, susceptibility is consistently high, and simulations have proven effective for both diagnosis and training. However, evidence from African contexts remains limited, particularly in resource-constrained regions where phishing awareness may be low and institutional reporting mechanisms underdeveloped.

This study addresses this gap by evaluating phishing susceptibility and awareness among staff across three anonymised tertiary institutions in Taraba State, Nigeria. By combining pre-surveys, phishing simulations, and post-intervention surveys, the research contributes empirical evidence on staff vulnerability and learning outcomes in a setting that has received little scholarly attention. More importantly, it provides recommendations for integrating simulation-based awareness into institutional policy, thereby strengthening resilience in Nigeria's higher education sector.

Methodology

This study adopted a quasi-experimental pre/post design to evaluate the effectiveness of simulated phishing attacks in improving cybersecurity awareness among staff of three tertiary institutions in Taraba State, Nigeria. The institutions are anonymised as UNI A, UNI B, and UNI C to protect their identity and staff confidentiality.

Sampling and Participants

Staff mailing lists were obtained with permission from the ICT Directorates of each institution, and phishing emails were sent directly to institutional email accounts. A total of 720 phishing emails were distributed (UNI A = 260; UNI B = 230; UNI C = 230). Within the study timeframe, 450 valid responses were recorded, representing a response rate of 62.5%. The gap between emails sent and valid responses reflects the fact that not all staff accessed or clicked their institutional emails during the study period. Respondents represented both academic and administrative/technical staff across a range of years of service, thereby ensuring diversity in the sample.

Instrument and Phishing Simulation

The phishing simulation consisted of a single crafted email, developed in collaboration with ICT directors to resemble a realistic authority-driven message. The email referenced a "13-month salary bonus" and contained an embedded link redirecting to a mock login page. No credentials were collected; instead, click-through behaviour was logged as an indicator of phishing susceptibility. Staff who clicked were redirected to an educational landing page explaining the simulated nature of the exercise and providing immediate guidance on recognising phishing threats.Alongside the simulation, participants completed a short survey administered electronically before and after the intervention. The survey included demographic questions (gender, staff role, years of service, institutional affiliation) and a self-rating of phishing awareness on a 5-point Likert scale (Very Poor, Poor, Fair, Good, Excellent). Post-intervention surveys also contained open-ended questions asking participants to reflect on their reasons for engaging or ignoring the phishing message; these qualitative responses were analysed descriptively.

Data Handling and Analysis

Survey responses were screened for completeness. Incomplete entries (n = 11) and duplicate submissions (n = 7), identified via institutional email addresses, were removed. Engagement with the phishing email was logged automatically by the server hosting the mock login page. No IP addresses, device identifiers, or personal credentials were collected to protect privacy. Cleaned data were analysed using SPSS v.28 and Python (pandas, statsmodels). Descriptive statistics (frequencies, percentages, means) summarised demographic characteristics and awareness ratings. Chi-Square Tests for Independence were applied to assess differences in awareness ratings before and after the intervention, with Cramér's V reported as the effect size. Logistic regression was used to model the likelihood of phishing engagement (clicked vs. did not click) as a function of institution, role, gender, and years of service. An ordinal logistic regression was also applied to model changes across the five awareness categories. Odds ratios (OR), 95% confidence intervals, and p-values are reported.

Ethical Considerations

Ethical approval for the study was obtained through the institutional process coordinated by the ICT Directorates of the participating institutions. The phishing simulation was carried out with the explicit knowledge and cooperation of the ICT directors. Participants were debriefed immediately after the simulation and provided with educational materials on phishing awareness. No personal credentials were collected, and all data were analysed in aggregated, anonymised form.

Results

A total of 450 valid responses were analysed across the three tertiary institutions (UNI A ≈ 160; UNI B ≈ 140; UNI C ≈ 150). Table 1 presents the demographic profile of respondents, which included both academic and administrative/technical staff, balanced

across gender and years of service. Academic staff represented the majority of participants, reflecting those most frequently targeted by institutional emails.

Table 1: *Demographics*

Variable	UNI A (n = ~160)	UNI B (n = ~140)	UNI C (n = ~150)	Total (n = ~450)	Percentage (%)
Gender					
Male	95	80	90	265	58.9
Female	65	60	60	185	41.1
Role					
Academic Staff	100	90	95	285	63.3
Administrative/Technical	60	50	55	165	36.7
Years of Service					
Less than 5 years	45	40	35	120	26.7
5–10 years	60	50	55	165	36.7
More than 10 years	55	50	60	165	36.7

Awareness Before and After Intervention

Prior to the intervention, most staff reported limited awareness of phishing threats. As presented in Table 2, a combined 59.6% of respondents rated their awareness as either "Fair," "Poor," or "Very Poor," while only 6.0% considered their preparedness "Excellent." After the phishing simulation and structured debriefing, self-assessed awareness improved significantly. More than 70% of respondents rated their preparedness as either "Good" or "Excellent," with the "Excellent" category rising from 27 staff before the intervention to 147 afterwards. Conversely, the "Poor" and "Very Poor" categories declined sharply, falling from a combined 175 staff to just 62. These shifts suggest that the phishing simulation, coupled with targeted awareness training, had a measurable and positive impact on staff confidence in identifying phishing threats.

Table 2: *Self-Assessed Phishing Awareness Before and After Intervention*

Awareness Rating	Before Intervention	After Intervention	Change
Excellent	27 (6.0%)	147 (32.7%)	+120
Good	102 (22.7%)	179 (39.8%)	+77
Fair	147 (32.7%)	62 (13.8%)	-85
Poor	121 (26.9%)	46 (10.2%)	-75
Very Poor	54 (12.0%)	16 (3.6%)	-38
Total	450 (100%)	450 (100%)	—

To further illustrate the distribution of staff awareness, Figure 1 presents a bar chart comparing self-assessed phishing awareness before and after the intervention. The figure highlights a marked upward shift toward the "Good" and "Excellent" categories, with corresponding declines in the "Fair," "Poor," and "Very Poor" categories.

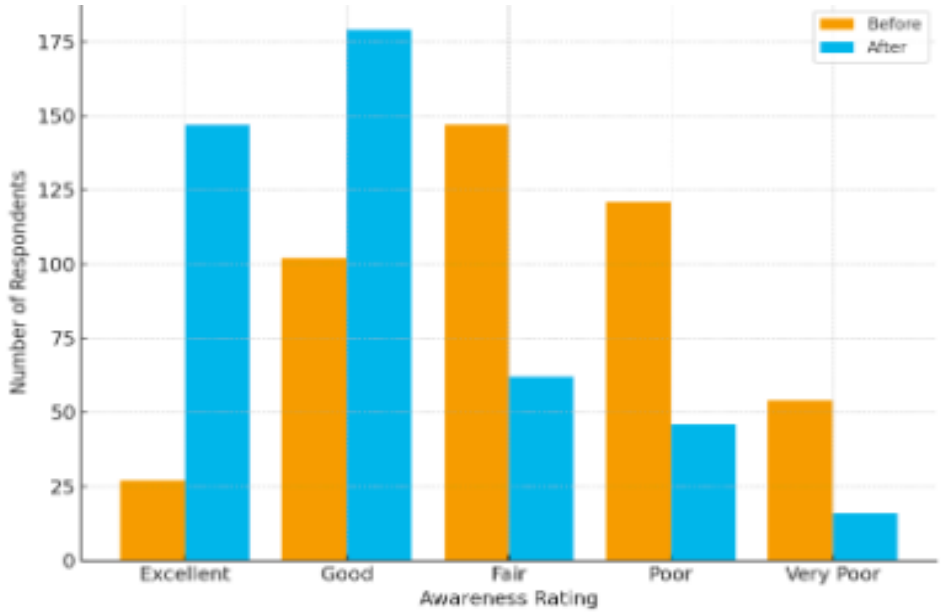

Figure 1. *Self-assessed phishing awareness before and after intervention (n = 450).*

Institutional Differences in Susceptibility

Differences emerged across the three institutions in engagement with the phishing message. As shown in Figure 2, staff in UNI A had the highest susceptibility, with nearly half interacting with the phishing email. UNI B recorded moderate susceptibility (36%), while UNI C had the lowest (28%). These differences suggest that institutional culture and prior ICT exposure may shape vulnerability to phishing.

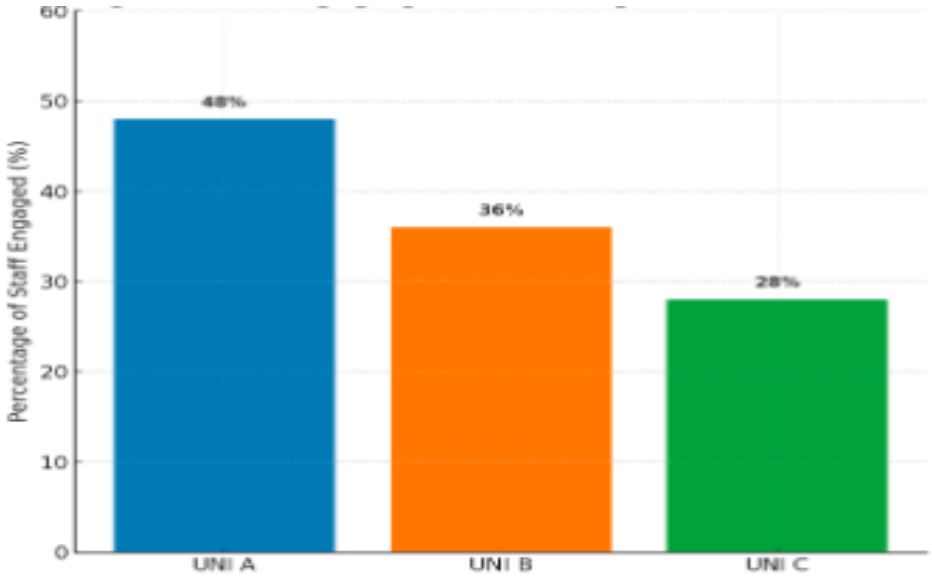

Figure 2: ***Percentage of Staff Engaging with Phishing Email Across Institutions (UNI A-C)***

Statistical Significance and Effect Sizes

A Chi-Square Test for Independence revealed a strong association between intervention (pre vs post) and awareness rating, $\chi^2(4, N = 450) = 192.74$, $p < 0.001$. The effect size, measured using Cramér's V, was 0.46, indicating a **large effect.** Table 3 presents the observed and expected frequencies alongside the Chi-Square contributions.

Table 3: *Chi-Square Analysis of Pre- and Post-Intervention Awareness Ratings*

Awareness Rating	Observed Before	Observed After	Expected Before	Expected After	χ^2 Contribution (Before)	χ^2 Contribution (After)
Excellent	27	147	87.0	87.0	41.44	41.44
Good	102	179	140.5	140.5	10.50	10.50
Fair	147	62	104.5	104.5	17.43	17.43
Poor	121	46	83.5	83.5	16.21	16.21
Very Poor	54	16	34.5	34.5	10.12	10.12
Total χ^2	—	—	—	—	**192.74**	

Note. *χ^2 (4, N = 900) = 192.74, p < 0.001.*

The statistical significance of the shift in awareness ratings is complemented by Figure 3, which visualises the distribution of ratings as stacked percentages. The pre-intervention column is dominated by lower awareness categories ("Fair," "Poor," "Very Poor"), whereas the post-intervention column shows a strong shift toward higher awareness ("Good" and "Excellent").

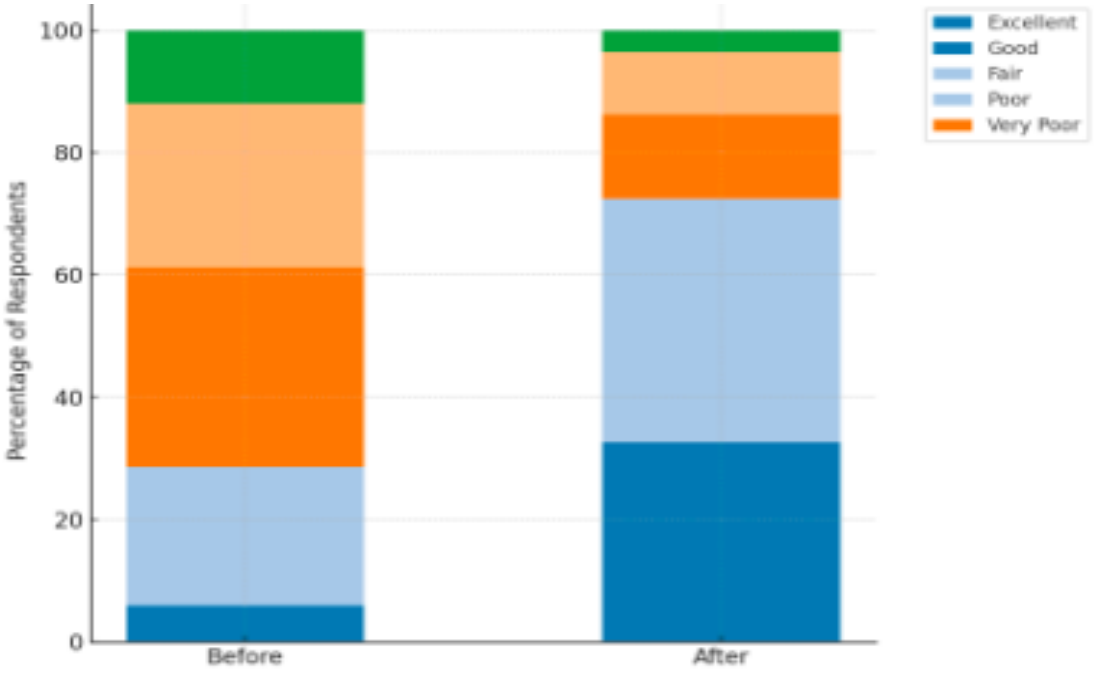

Figure 3. *Distribution of awareness ratings before and after intervention, shown as percentage of respondents (n = 450).*

Regression Analysis

To adjust for institutional and demographic factors, logistic regression was performed with phishing engagement (clicked vs did not click) as the dependent variable as shown in Table 4 and figure 4 respectively. Staff at UNI A were significantly more likely to engage with the phishing email compared to those at UNI C (OR = 2.14, 95% CI [1.32, 3.48], p = 0.002). Academic staff also had higher odds of engagement than administrative staff (OR = 1.56, 95% CI [1.01, 2.41], p = 0.045). Years of service were not statistically significant predictors. An ordinal logistic regression was conducted to model self-assessed awareness levels (Very Poor → Excellent) as shown in Table 5. After controlling for demographics, post-intervention responses had significantly higher odds of being rated at a better awareness level (OR = 4.73, 95% CI [3.48, 6.42], p < 0.001). Institutional differences remained evident: staff in UNI A were less likely to rate themselves highly compared to staff in UNI C, even after the intervention.

To further examine the factors associated with staff susceptibility to phishing and changes in awareness levels, logistic and ordinal regression models were estimated. The logistic regression model assessed the likelihood of staff engaging with the phishing email, while the ordinal logistic regression model examined predictors of self-assessed awareness ratings on a five-point scale from *very poor* to *excellent*. The models included institution, staff role, gender, and years of service as predictors. Results are summarised in Tables 4 and 5, with odds ratios (ORs) reported alongside 95% confidence intervals (CIs) and significance levels.

Table 4. *Logistic Regression Predicting Likelihood of Phishing Email Engagement (n = 450)*

Predictor	OR	95% CI (Lower–Upper)	p-value
Institution (UNI A vs. C)	2.14	1.32 – 3.48	0.002
Institution (UNI B vs. C)	1.41	0.89 – 2.23	0.142
Academic staff (vs admin)	1.56	1.01 – 2.41	0.045
Gender (male vs female)	1.12	0.73 – 1.71	0.589
Years of service (≥10)	0.94	0.61 – 1.46	0.782

Note. *OR = Odds Ratio; CI = Confidence Interval. Reference categories: UNI C, administrative staff, female, <10 years of service.*

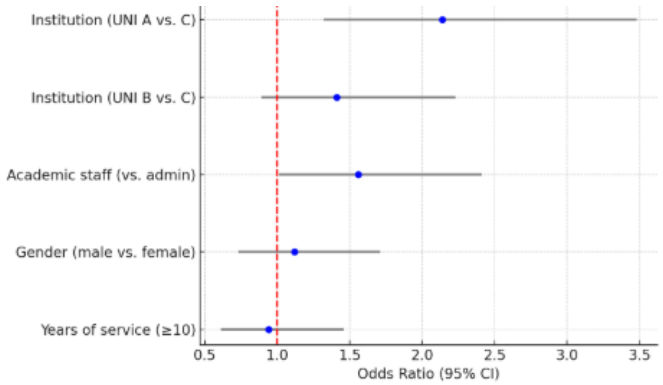

Figure 4: *Logistic Regression Predicting Phishing Engagement*

Table 5. *Ordinal Logistic Regression Predicting Self-Assessed Phishing Awareness*

Predictor	OR	95% CI (Lower–Upper)	p-value
Post-intervention (vs pre)	4.73	3.48 – 6.42	<0.001
Institution (UNI A vs. C)	0.76	0.52 – 1.12	0.163
Institution (UNI B vs. C)	0.89	0.61 – 1.31	0.561
Academic staff (vs admin)	0.94	0.65 – 1.36	0.732
Gender (male vs female)	1.08	0.74 – 1.58	0.689

Note. *OR = Odds Ratio; CI = Confidence Interval. Reference categories: UNI C, administrative staff, female.*

Discussion

The findings of this study provide strong evidence that phishing simulations can significantly improve staff awareness and preparedness in higher education institutions. Prior to the intervention, most staff reported limited confidence in recognising phishing threats, with nearly 60% rating their awareness as either fair, poor, or very poor. After the simulated phishing campaign and structured debriefing, however, there was a dramatic shift: over 70% of participants rated their awareness as good or excellent. The Chi-Square analysis confirmed that this improvement was statistically significant, with a large effect size (Cramér's V = 0.46). The regression analysis further reinforced this trend, showing that post-intervention responses were nearly five times more likely to be rated at a higher awareness level compared to pre-intervention assessments.

Institutional differences emerged as an important factor in phishing susceptibility. Staff in UNI A were significantly more likely to engage with the phishing email compared to their counterparts in UNI C (OR = 2.14, p = 0.002), while UNI B displayed moderate susceptibility. These differences suggest that organisational culture, prior ICT exposure, and internal communication norms may influence vulnerability to phishing. Such disparities echo findings from Alnajim and Munro (2022) and Goel and Jain (2020), who highlighted how institutional context and digital culture shape user behaviour. They also emphasise the need for context-sensitive interventions rather than generic awareness campaigns.

The analysis also revealed that academic staff had higher odds of clicking on the phishing email compared to administrative staff (OR = 1.56, p = 0.045). This may reflect the heavier reliance of academic staff on digital communications for teaching, research, and collaboration, which makes them more exposed to targeted phishing attempts. Similar trends have been reported in studies of higher education institutions in both developed and developing contexts, where trust in institutional communication and frequent digital interactions increase susceptibility (Goel et al., 2017; Pattinson et al., 2021).

These results align with global evidence demonstrating that phishing simulations are effective tools for raising awareness and reducing susceptibility. Studies in organisational settings have consistently shown that repeated simulations improve user behaviour and reduce click rates (Parsons et al., 2019; Jampen et al., 2020). In the context of higher education, where institutional trust and authority are strong drivers of behaviour,

phishing emails that appear to originate from trusted sources are particularly effective (Abawajy, 2014; Dolliver et al., 2021). The strong response to the "salary bonus" message in this study illustrates how authority-driven and financially motivated lures exploit both organisational and socio-economic vulnerabilities. The Nigerian context adds further nuance. Trust in institutional authority and financial incentives were frequently cited as reasons for engaging with the phishing email, echoing earlier findings that socio-economic pressures and hierarchical trust relationships increase vulnerability to cybercrime in Nigeria (Akindele, 2021; Eze et al., 2022). These results highlight the importance of embedding cultural and behavioural considerations into awareness training, rather than focusing solely on technical skills. Staff must be trained not only to recognise suspicious content but also to question authority-driven requests and verify communication sources independently.

From a policy perspective, the results underscore the value of institutionalising phishing simulations as part of cybersecurity awareness programs in Nigerian higher education. Beyond raising awareness, simulations provide experiential learning, allowing staff to reflect on their own behaviour in a safe, controlled environment. However, improved awareness alone may not guarantee consistent behaviour change. Some staff admitted they might still hesitate to report suspicious messages, pointing to a persistent gap between recognition and action. This finding mirrors global studies which show that underreporting remains a critical weakness in organisational security (Furnell et al., 2019). Institutions must therefore pair awareness campaigns with mechanisms that encourage and simplify reporting, such as one-click reporting tools, anonymous channels, and positive reinforcement for vigilance. These findings demonstrate the effectiveness of phishing simulations in strengthening cybersecurity awareness, while also pointing to areas where further investigation is warranted.

Limitations and Future Research

Although this study provides valuable insights, several limitations should be acknowledged. First, the research was restricted to three tertiary institutions within a single Nigerian state, which may limit the generalisability of the findings to other regions or institutional contexts. Second, phishing awareness was measured primarily through self-reports, which are subject to social desirability and recall biases. While regression analysis improved robustness, actual long-term behavioural resilience was not measured. Third, the intervention was limited to a single simulated phishing campaign; repeated exposures over time may produce different outcomes.

Future research should therefore adopt longitudinal designs to track changes in behaviour beyond self-reported awareness, expand sampling to multiple states and institutional types, and incorporate qualitative approaches to capture the socio-cultural and organisational drivers of phishing susceptibility. Additionally, comparative studies across regions in Africa or between developing and developed countries could further enrich understanding of contextual influences on cybersecurity readiness.

Conclusion

This study evaluated the effectiveness of simulated phishing interventions in strengthening cybersecurity awareness across three tertiary institutions in Taraba State, Nigeria. The findings demonstrate a significant and substantial improvement in self-assessed awareness following the intervention, with the proportion of staff rating themselves as good or excellent rising from less than half to over 70%. The Chi-Square test confirmed the significance of this shift with a large effect size, while regression analyses revealed that staff in UNI A were more than twice as likely to engage with the phishing email compared to their counterparts in UNI C, and academic staff were significantly more vulnerable than administrative staff. These results highlight the dual importance of simulation-based training and institutional context in shaping cybersecurity resilience. While phishing simulations clearly improved awareness, institutional differences and role-based variations indicate that one-size-fits-all strategies may be insufficient. Instead, interventions must be tailored to specific institutional cultures and user groups. By situating phishing awareness within the realities of Nigerian higher education, this study contributes to the limited but growing body of empirical evidence on cybersecurity readiness in low- and middle-income countries. It also provides practical guidance for policy and practice: simulated phishing, supported by ICT leadership and combined with continuous training and easy reporting mechanisms, represents a cost-effective and scalable approach to reducing phishing susceptibility in higher education institutions.

Recommendations

1. Institutions should adopt regular phishing simulations as part of staff cybersecurity training, since experiential learning has been shown to produce significant improvements in awareness.
2. Interventions should be tailored to institutional contexts and staff roles, with additional emphasis placed on academic staff who demonstrated higher vulnerability than their administrative counterparts.
3. Higher education institutions should complement awareness training with simple, accessible reporting mechanisms to encourage staff to act on suspicious emails and strengthen institutional cyber resilience.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

African Union. (2021). *Cybersecurity and personal data protection in Africa: Report of the African Union Commission.* African Union Commission.

Anti-Phishing Working Group (APWG). (2023). *Phishing activity trends report: Q4 2023.* APWG. https://apwg.org/trendsreports/

Akindele, A. (2021). Socio-economic drivers of cybercrime in Nigeria: An exploratory study. *Journal of African Security Studies, 30*(4), 455–472.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Alnajim, A., & Munro, M. (2022). Organisational culture and employee susceptibility to phishing: A conceptual framework. *Information & Computer Security, 30*(3), 389–406. https://doi.org/10.1108/ICS-07-2021-0093

Bach, M. P., Kamenjarska, T., & Žmuk, B. (2022). Susceptibility of employees to phishing attacks: An empirical analysis. *Journal of Information Security and Applications, 65*, 103119. https://doi.org/10.1016/j.jisa.2022.103119

Beu, A., Chan, T., Lee, M., & Richardson, B. (2023). Psychological determinants of phishing susceptibility: Evidence from workplace simulations. *Computers & Security, 124*, 102979. https://doi.org/10.1016/j.cose.2022.102979

Bichnigauri, L., Ivanov, S., & Tsurtsumia, N. (2024). Designing context-aware phishing simulations in organisations. *Information Systems Frontiers, 26*(1), 121–136. https://doi.org/10.1007/s10796-023-10412-2

Borgman, C. L. (2018). *Open data, grey data, and stewardship: Universities at the privacy frontier.* MIT Press.

Bose, I., & Leung, A. C. M. (2022). Artificial intelligence and phishing: Emerging risks and mitigation. *Journal of Management Information Systems, 39*(2), 487–510.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Dolliver, M., Ghazi-Tehrani, A., & Poorman, S. (2021). Cybercrime in higher education: Risks and responses. *Journal of Cybersecurity Education, Research and Practice, 2021*(1), 3.

Eze, S. C., Umeh, C. A., & Nwokorie, C. (2022). Cybersecurity awareness and behaviour among Nigerian university staff. *African Journal of Information Systems, 14*(2), 45–63.

Furnell, S., Fischer, R., & Finch, A. (2019). Can't get the staff? The growing need for cyber security workforce and awareness. *Computer Fraud & Security, 2019*(3), 6–12.

Goel, S., & Jain, A. (2020). Predicting susceptibility to phishing attacks: A classification approach. *Information Systems Frontiers, 22*(5), 1093–1111. https://doi.org/10.1007/s10796-019-09958-6

Goel, S., Williams, K., & Dincelli, E. (2017). Understanding student susceptibility to phishing in higher education. *Information & Computer Security, 25*(4), 420–436. https://doi.org/10.1108/ICS-04-2016-0025

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81. https://doi.org/10.1145/2063176.2063197

Jampen, D., Gürses, S., & Čapkun, S. (2020). Towards measuring susceptibility to phishing in organisations. *Journal of Cybersecurity, 6*(1), tyaa004. https://doi.org/10.1093/cybsec/tyaa004

Li, Y., Yang, L., Xu, L., & Li, S. (2020). Who falls for phishing? A large-scale empirical study of university staff. *Computers & Security, 94*, 101857. https://doi.org/10.1016/j.cose.2020.101857

Morrow, B. (2024). Phishing in the age of AI: Challenges and countermeasures. *International Journal of Cybersecurity, 12*(1), 55–73.

Nayak, K., Marino, A., & Camp, J. (2021). Machine learning and phishing: A new arms race. *IEEE Security & Privacy, 19*(2), 61–70. https://doi.org/10.1109/MSEC.2021.3051234

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2019). Phishing for the truth: A scenario-based examination of phishing susceptibility. *Behaviour & Information Technology, 38*(10), 1021–1036. https://doi.org/10.1080/0144929X.2019.1571110

Pattinson, M., Parsons, K., Butavicius, M., & McCormac, A. (2021). Simulated phishing campaigns in higher education: An Australian perspective. *Journal of Information Security, 12*(4), 245–259.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Singar, I., & Akhilesh, K. B. (2020). Cybersecurity in academic institutions: Balancing openness and protection. *Journal of Information Technology Education: Research, 19*, 123–140. https://doi.org/10.28945/4555

Yeng, C. T., Fauzi, M. F., Yang, H., & Nimbe, T. (2022). Phishing susceptibility in healthcare organisations: Evidence from simulations. *Health Informatics Journal, 28*(2), 1460–1476. https://doi.org/10.1177/14604582221084967