www.ijarp.com ISSN 2456-9992 Page: 01-15
International Journal Advanced Research Publications
Research Article
Volume: 02
Issue: 07

EVALUATING THE EFFECTIVENESS OF PHISHING SIMULATIONS IN ENHANCING CYBERSECURITY AWARENESS AMONG ACADEMIC STAFF: EVIDENCE FROM A NIGERIAN POLYTECHNIC

Husseini Usman Yaro,[1*] Augustine Ndudi Egere[2]

ICT Unit, Federal Polytechnic Bali, Taraba State, Nigeria.

Department of Computer Science, Federal Polytechnic Bali, Taraba State, Nigeria.

Article Received: 26 May 2026, Article Revised: 14 June 2026, Published on: 04 July 2026

***Corresponding Author: Husseini Usman Yaro**

ICT Unit, Federal Polytechnic Bali, Taraba State, Nigeria.

Doi: https://doi-doi.org/101555/ijarp.9415

ABSTRACT

Phishing attacks remain one of the most prevalent and damaging cybersecurity threats to organizations, particularly academic institutions that manage vast amounts of sensitive data. This study assesses the effectiveness of a targeted cybersecurity awareness intervention conducted among staff from four academic schools at Federal Polytechnic Bali. Utilizing a quasi-experimental design, the research involved a pre-awareness survey, a simulated phishing email themed around a "13-month bonus payment," and a post-intervention survey to evaluate changes in phishing awareness and response behaviours. Results revealed a high initial susceptibility, with 66.5% of participants falling for the phishing simulation, particularly from the Schools of Science and Technology (SST) and Business and Management Technology (SBMT). However, post-intervention assessments demonstrated a statistically significant improvement in participants' self-assessed cybersecurity knowledge, as confirmed by a Chi-Square Test for Independence ($\chi^2 = 72.43$, $p < 0.0001$). The study highlights the critical need for continuous, customized awareness training and a proactive incident reporting culture to strengthen institutional resilience against phishing threats.

KEYWORDS: Cybersecurity, Phishing Simulation, Awareness, Education, Academic Institution, and Staff Training.

INTRODUCTION

In today's digital environment, cybersecurity threats pose substantial difficulties to all types of organizations. Even though larger organizations often employ IT teams and cybersecurity

experts to handle these challenges. However, someorganisations frequently lack the means and skills to fully protect themselves from cybersecurity threats. Among the various cyber threats, phishing attacks remain one of the most common and effective methods that hackers use to access private information and disrupt organizational operations (Mercuri, D. 2025). Phishing attacks use human psychology to manipulate, frequently deceiving people into disclosing valuable information or compromising security systems. As a result, improving cybersecurity resilience against such assaults has become critical for institutions seeking to secure their assets while maintaining operational integrity. Phishing tactics have changed over time, becoming increasingly complex and difficult to detect. Attackers use social engineering techniques to construct very convincing emails, texts, and websites that impersonate legitimate organisations. Considering this, even the most attentive staff may succumb to these deceitful methods (Sharif 2024). One of the most important parts of an organization's defences against phishing is cybersecurity awareness training. The goal of the training is to provide staff with the information and skills to identify, prevent, and report phishing attacks (Iqbal and Yusof, 2024). The advent of advanced technologies, such as machine learning and artificial intelligence, has further amplified the threat, enabling attackers to create compelling and personalized phishing campaigns (Jimmy, 2021). The School of Science and Technology at Federal Polytechnic Bali, like many institutions, faces growing risks posed by phishing attacks targeting its staff. These attacks exploit human vulnerabilities more than technological loopholes, underscoring the critical need for comprehensive cybersecurity awareness programs. This studyaims to assess the effectiveness of targeted awareness efforts in equipping staff with the knowledge and skills to recognize, resist, and report phishing attempts. By evaluating the current level of awareness and the impact of simulated phishing exercises, the research seeks to identify gaps, measure behavioural changes, and recommend strategic interventions for enhancing institutional resilience. Ultimately, the goal is to create a more secure digital environment that supports the institution’s academic mission while safeguarding its technological infrastructure.

Literature Review

Phishing refers to a deceptive tactic where attackers mimic legitimate websites to trick individuals into revealing sensitive information such as login credentials, financial details, or personal data. These attacks commonly manipulate users into performing specific actions desired by the attacker. They intersect elements of social engineering, technology, security practices, and even political considerations. Typically, phishing attempts are delivered

through messages, most often emails, that appear to originate from trusted sources (Hillman, Harel, & Toch, 2023).

Phishing continues to evolve as a prominent cyber threat, targeting a wide range of users across different socio-demographic groups. In a study by Bach, Kamenjarska, and Žmuk (2022), the researchers investigated the profiles of individuals most likely to be targeted by phishing attacks. Their findings challenge the common assumption that individuals with higher educational levels are less susceptible to phishing attacks. Surprisingly, their results indicated that individuals with higher education were more susceptible to phishing attacks.

According to the 2020 Anti-Phishing Working Group (APWG) report, the number of phishing websites discovered rose between Q4 2019 and Q1 2020. Moreover, there were around 214,345 distinct phishing sites, and recent phishing assaults have increased since early 2020 and in the year 2021, 83% of institutions reported phishing assaults. In a recent report, APWG's Q4 2023 Phishing Activity Trends Report discloses that the APWG study carefully examines precariously close to five million phishing attacks in 2023, making it a breaking-record year for phishing. APWG Senior Research Fellow highlights that phishing attacks dropped in the mid-year of 2023 because of the termination of operation of the free assessable domain name program called Freenom. However, despite a decline in the first quarter, phishing increased in the latter half of the year. In the final phase of 2024, the APWG noticed 1,007,501 phishing attacks.

According to Beu et al. (2023), organizations evaluate employee susceptibility to phishing attacks by conducting regular blinded phishing simulation exercises. These phishing simulations involve sending emails to employees with identifiable phishing cues, such as suspicious sender URLs or spelling errors. Key metrics derived from these simulations are click rate and reporting rate. Click rate displays the percentage of successful phishing attempts by the employees to click the link in an illegitimate email. On the other hand, the reporting rate reflects the percentage of simulated phishing links that were reported using the organization's reporting process for suspected phishing emails, demonstrating proactive awareness of potential threats. In research by Yeng et al. (2022), involving 167 healthcare staff in phishing simulations, 102 (61.1%) engaged with the simulated malicious link, while 65 (38.9%) remained unaffected by the attack. Additionally, 25 participants (24.5%) out of the 102 who visited the link completed the questionnaire included in the research. Thus, 77 people (75.5%) did not respond to the survey. The clicking behaviour was increased at the beginning of the simulated attack but significantly reduced after the initial two days. Among the 167 staff members who received the simulated phishing email, 61.1% fell victim.

Nevertheless, just 25 (24.5%) of the victims completed a questionnaire, citing various reasons for their vulnerability. For example, 7 (68%) of the 25 participants trusted the phishing message's subject, whereas 6 (24%) were inquisitive.

Phishing in Academic Institutions

Morrow (2024) highlights that a solitary academic institution may endure millions of cyberattacks weekly. Phishing attackers may want to get confidential information, intellectual property, or financial data. Higher education institutions frequently handle substantial quantities of personally identifiable information on students and workers, which may be exploited for illicit activities such as identity theft or extortion. Singar et al. (2020) noted that educational institutions have extremely comprehensive and intricate online activities concerning the wide range of data they own and their assortment of actions on the internet, accumulating computing power. In the field of cybersecurity, an educational institution is not simply another susceptible organisation; various elements make the organisation a unique cybersecurity target.

According to Borgman (2018), educational institutions that have integrated digital technology in all aspects of their operations have a continuous procedure for generating and utilizing data obtained from registrars, faculty documents, identity cards used for permission services, etc. Additionally, by using EdTech to gather as much data as possible on students and their academic grades, big data analytics and educational data mining are being used to enhance instructional materials and assist teachers in understanding the unique requirements of each student. Students' privacy has long been a source of worry for such data-gathering activities. As colleges become more vulnerable to cyberattacks, security becomes even more of a problem because of the enormous volume of different data that is difficult to safeguard.

Li et al. (2020) draw attention to the fact that universities are experiencing cyberattacks, with a minimum of one out of three simulated phishing emails being clicked by more than 20% of university staff. A broadly similar point has also been made by Goel et al. (2017), who found that a substantial number of students, approximately over 25% opened phishing, and half of them took a risk by clicking the attached link. This leads to security breaches and other cybersecurity incidents. In the same vein, Dolliver et al. (2021) outline that universities frequently deal with large volumes of sensitive information about staff and students, which can be traded or utilized for criminal activities, including identity theft or extortion. As a result, a single university is subject to a massive number of cyberattacks weekly.

Impact of Phishing Simulation

There is a growing body of literature that recognizes the importance of phishing simulation in an organization. Several organizations implement phishing simulations as a preventative defensive strategy in response to the increasing sophistication of phishing attacks. By simulating genuine phishing scenarios, these simulations enable organizations to evaluate the awareness levels as well as the responses of their staff members. Phishing simulations are effective educational instruments that extend beyond evaluation. They foster a culture of increased awareness among staff members, providing them with the essential skills necessary to recognize and thwart phishing attempts. The successful implementation of phishing simulation necessitates the customization of scenarios to reflect the organization's actual hazards. These simulations, which vary in complexity, offer tools to improve comprehension of phishing indications as well as instant feedback. Employees get an acute sense of phishing red flags through frequent simulations, which improves their capacity to identify and neutralize such threats (Bichnigauri et al., 2024).

METHODOLOGY

This study employed a quasi-experimental design involving a pre-survey, a controlled phishing simulation, and a post-survey to assess phishing awareness among staff from four academic schools at Federal Polytechnic Bali—SST, SET, SAT, and SBMT. A total of 270 staff were purposively selected, and data were collected in three phases: the pre-survey measured baseline cybersecurity knowledge, the phishing simulation involved sending a deceptive email themed around a “13-month bonus payment,” and the post-survey evaluated participants’ responses, experiences, and awareness gains. Instruments included structured questionnaires and a monitored phishing email, with data analyzed using descriptive statistics and a Chi-Square Test for Independence to assess changes in self-assessed knowledge. Ethical considerations were consistently observed, with participant anonymity maintained, and a post-simulation debriefing conducted to explain the exercise and reinforce cybersecurity education.

RESULTS

This section presents the outcomes of the phishing simulation study and the comparative analysis of cybersecurity awareness among selected academic schools at Federal Polytechnic Bali (FPB), namely the School of Science and Technology (SST), School of Engineering Technology (SET), School of Agricultural Technology (SAT), and the School of Business and

Management Technology (SBMT). The analysis integrates results from pre- and post-simulation surveys and simulation performance data.

Pre-Simulation Awareness Across Schools

A total of 168 responses were received out of the 200 distributed questionnaires, representing a response rate of 84%. Analysis of the academic school categories revealed that SETcontributed 38 respondents (19%), SAT contributed 35 (17.5%), SST recorded 50 (25%), and SBMT recorded 45 (22.5%). These proportions reflect fairly equitable participation across the four schools, ensuring representativeness in measuring baseline cybersecurity awareness. This is depicted in Figure 1 below.

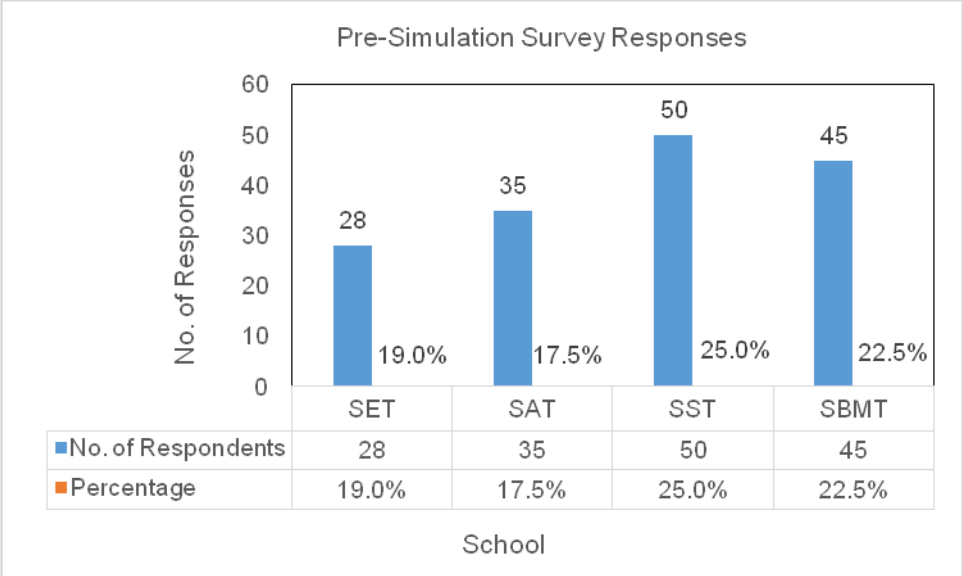

Figure 1: Pre-Simulation Survey Responses.

Before the simulation, a significant portion of the respondents demonstrated limited familiarity with core cybersecurity concepts. Only 32.6% of staff reported familiarity with cybersecurity, while the majority (67.4%) had not received any form of cybersecurity training as shown in Figure 2.

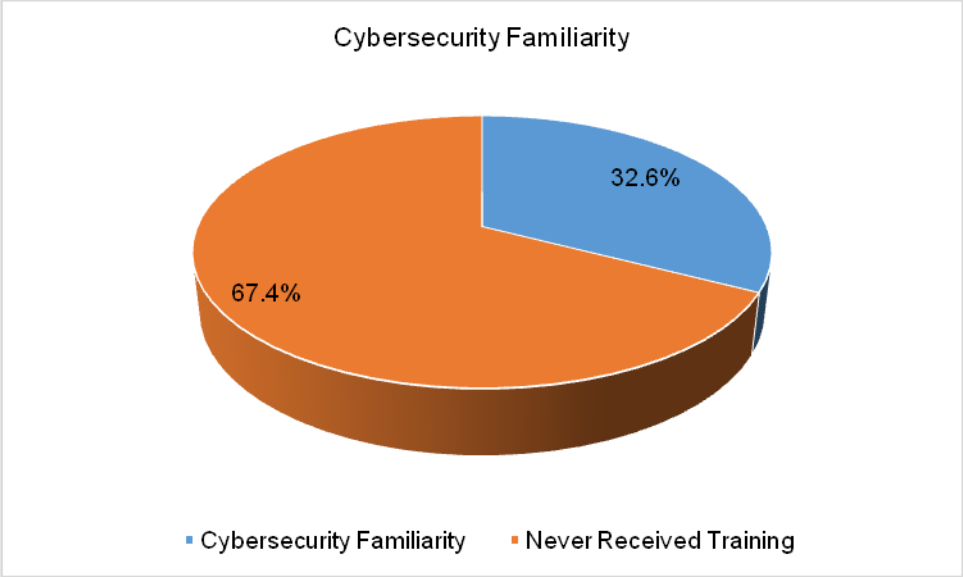

Figure2: Cybersecurity Familiarity.

Furthermore, Figure 3 below shows the awareness of phishing threats was generally low, with 32.7 respondents rating their knowledge as "Fair" and an additional 26.8% describing it as "Poor"and 11.9% as “Very Poor”. This highlights the urgent need for targeted cybersecurity awareness programs within these academic units.

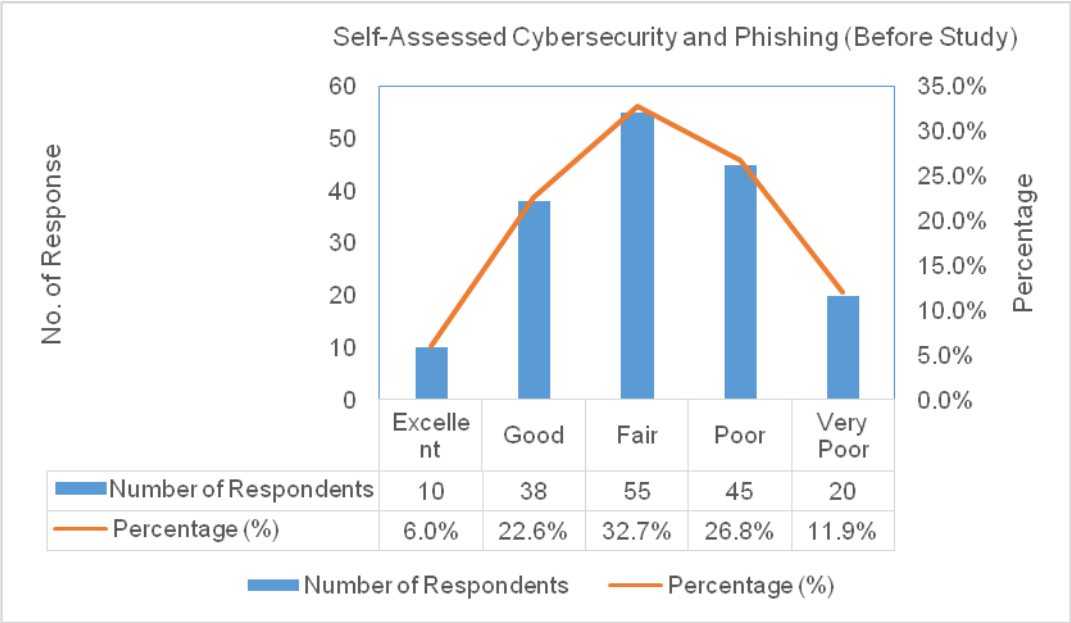

Figure3: Self-Assessed Cybersecurity and Phishing. (Before Study)

Phishing Simulation Performance by School

During the phishing simulation phase, 270 phishing emails were disseminated. The results showed that 133 recipients (66.5%) clicked on the link and submitted their data. Among the

four academic schools under review, SST staff had the highest rate of successful phishing submissions at 42 (21.0%), followed by SBMT with 35 (17.5%). SAT recorded 30 submissions (15.0%), while SET had the lowest among the group at 26 (13.0%) as illustrated in Figure 4.

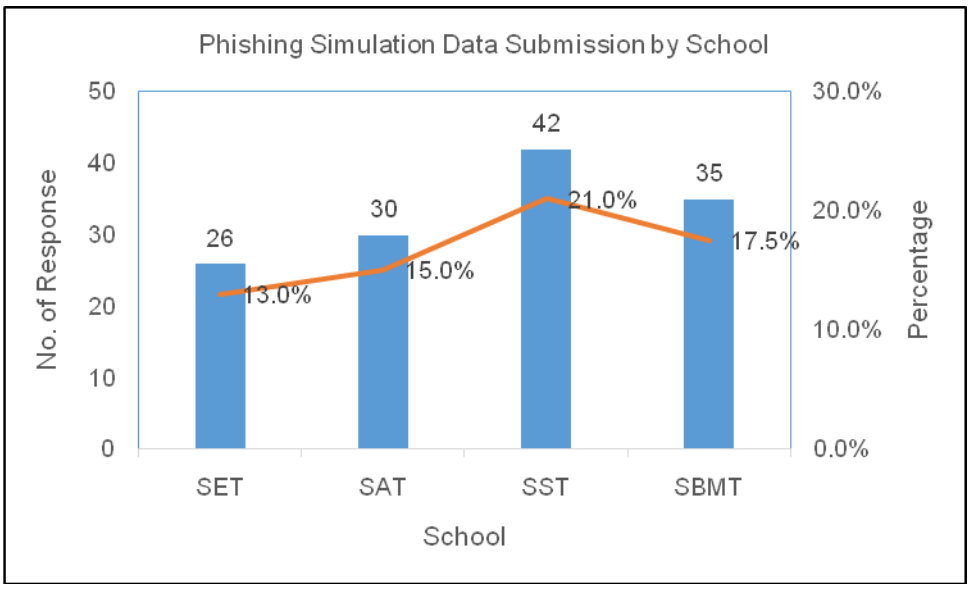

Figure4: Phishing Simulation Data Submission by School.

This distribution indicates that staff from SST and SBMT were comparatively more susceptible to phishing attacks than their counterparts inSAT and SET. These differences may be attributed to variation in job roles, email engagement levels, or perhaps differing levels of exposure to phishing awareness materials. The phishing email themed around a "13-month bonus payment" appears to have effectively exploited the recipients' expectations and trust in internal communication.

Post-Simulation Survey Insights

The post-simulation survey further revealed that the phishing attempt was widely recognized among the participants. A substantial number admitted to engaging with the email in various forms. Notably, over 70% of those who responded admitted to clicking the embedded link, while some acknowledged taking additional actions, such as reporting or deleting the email. However, a segment of staff also admitted to taking no action despite identifying the message as a phishing attempt, indicating lapses in proactive threat response behaviour.

Respondents who were deceived by the phishing email cited institutional trust, urgency in communication, and the financial theme of the message as primary factors influencing their decision to engage. Specifically, 98.4% stated they trusted the email because it appeared to

originate from the institution, while 95.1% were motivated by the financial incentive in the subject line. This underscores the psychological dimension of phishing effectiveness, especially when tailored to mimic institutional communication and offer appealing incentives.

Conversely, respondents who avoided the phishing trap indicated that they relied on various clues, such as grammatical errors (85.1%), sense of urgency (83%), and suspicious links (66%). This indicates some level of phishing literacy among a segment of staff, though the overall susceptibility rate remains concerning.

Impact of Simulation on Awareness

The post-intervention self-assessment data reveal a significant positive trend, suggesting the intervention's success in enhancing cybersecurity awareness and phishing detection skills among the target population.

Figure 5 illustrates the distribution of participants' self-assessed cybersecurity and phishing awareness levels following the awareness intervention. Out of a total of 168 respondents, the majority rated their knowledge and preparedness as "Good" (67 respondents, 39.9%) and "Excellent" (55 respondents, 32.7%). This suggests a high level of confidence among participants in their ability to identify and respond to phishing threats following completion of the awareness program. A smaller portion of the respondents rated their competency as Fair (23 respondents, 13.7%), while only 17 (10.1%) and 6 (3.6%) assessed their awareness as Poor and Very Poor, respectively. The relatively low percentages in these latter categories may indicate that the intervention effectively addressed existing knowledge gaps and improved participants' perception of their cybersecurity capabilities.

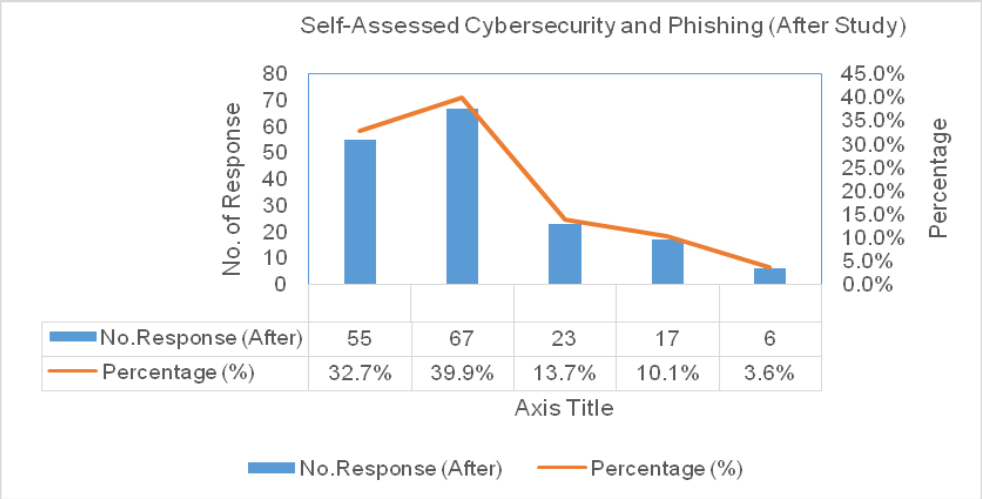

Figure 5: Self-Assessed Cybersecurity and Phishing. (After Study)

Pre- and Post-Study Evaluation of Participants' Cybersecurity Self-Ratings

Figure 6 illustrates the changes in participants' self-assessment of their cybersecurity knowledge before and after the study. Initially, most participants rated themselves as "Fair" (32.7%) and"Poor" (26.8%), with only a small proportion considering their knowledge to be Excellent (6.0%). However, following the study, there was a marked improvement in self-perception, as evidenced by a significant increase in "Excellent" ratings to 32.7% and "Good" ratings to 39.9%. Conversely, the percentages of participants rating themselves as Fair, Poor, or Very Poor dropped substantially. These shifts suggest that the study positively influenced participants' confidence in their cybersecurity awareness. The distribution of responses before and after the intervention highlights a clear upward trend in self-assessed competence, indicating the effectiveness of the awareness program.

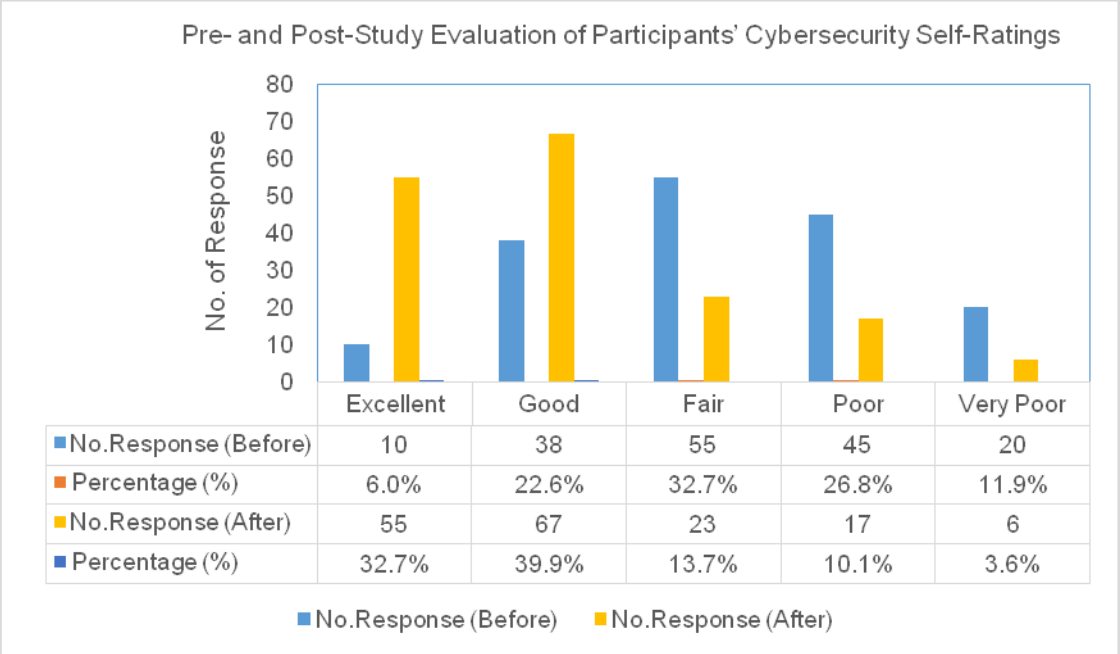

Figure 6: Pre-and Post-Study Evaluation of Participants' Cybersecurity Self-Ratings.

The Chi-Square Test for Independence can be applied to examine the variation in participants' self-assessment ratings before and after the study. This statistical method helps to determine whether the differences in rating distributions are significant. Table 1 presents the expected values for the assessment ratings recorded before and following the simulation.

Table 1: Pre- and Post-Study Evaluation Self-Ratings.

Scale	Before	After	Row Total
Excellent	10	55	65
Good	38	67	105

Fair	55	23	78
Poor	45	17	62
Very poor	20	6	26
	168	**168**	**336**

Chi-Square Test Analysis of Self-Assessment Ratings

To determine whether there was a statistically significant change in participants' self-assessed cybersecurity knowledge before and after the simulation, a Chi-Square Test for Independence was conducted. Table 2 presents the expected frequencies alongside the calculated Chi-Square components for each rating category.As shown, the expected frequencies for both pre- and post-study responses were computed under the assumption of independence, using the formula:

$$E = \frac{RT \times CT}{GT}$$

where RT is row total, CT is the column total and GT is the grand total

$$E = \frac{65 \times 168}{336} = 32.5$$

Using the above method, the complete set of expected frequencies is shown in Table 2 below.

Table 2: Expected Self-Assessment Ratings.(Pre- and Post-Simulation)

Scale	Excellent	Good	Fair	Poor	Very Poor	Total
Before	32.5	52.5	39	31	13	168
After	32.5	52.5	39	31	13	168
						336

The Chi-Square value for each cell was obtained as shown in Table 3 by applying the formula:

$$\chi^2 = \frac{(O - E)^2}{E}$$

where O represents the observed frequency and E the expected frequency.

To determine whether there was a significant change in participants' self-assessment of their knowledge before and after the phishing simulation, a Chi-Square Test for Independence was conducted. The expected frequencies (E1 for pre-simulation and E2 for post-simulation) were calculated, and the observed differences between the pre- and post-simulation ratings were analyzed. The table below summarizes the contributions of each response category to the total Chi-Square value.

Table 3:Chi-Square Contributions by Rating Scale.

Scale	Pre-study	Post-study	EB (E_1)	EA (E_2)	$\frac{(O_1 - E_1)^2}{E_1}$	$\frac{(O_2 - E_2)^2}{E_2}$	Chi-Square contributions
Excellent	10	55	32.5	32.5	15.57	15.57	31.14
Good	38	67	52.5	52.5	4.00	4.01	8.01
Fair	55	23	39	39	6.56	6.56	13.12
Poor	45	17	31	31	6.32	6.32	12.64
Very poor	20	6	13	13	3.76	3.76	7.52

The contributions of each rating scale to the overall Chi-Square statistic are presented in the final column. The "Excellent" category exhibited the highest contribution (χ^2 = 31.14), reflecting a substantial increase in the number of participants who rated their cybersecurity knowledge as "Excellent" following the simulation. Similarly, notable shifts were observed in the "Fair" (χ^2 = 13.12) and "Poor" (χ^2 = 12.64) categories, further indicating changes in perceived competency.

Computation of the Chi-Square Statistic

The Chi-Square statistic was calculated using the standard formula:

$$X^2 = \sum \frac{(O - E)^2}{E}$$

A significance level of 0.05 was chosen, as it is commonly adopted in research for hypothesis testing.

Substituting the observed and expected values into the formula yields:

$$X^2 = \sum \frac{(O - E)^2}{E}$$

$$X^2 = \sum \frac{(O - E)^2}{E} = 7.52 + 12.64 + 13.12 + 8.01 + 31.14 = 72.43$$

Given that the analysis involves two groups (pre- and post-study) across five rating categories, the degrees of freedom (df) are calculated as:

$$Degree\ of\ freedom\ (df) = (2 - 1) \times (5 - 1) = 4$$

Hypothesis

Null Hypothesis (H_0): Self-assessment ratings remained unchanged before and after the study.

Alternative Hypothesis (H_1): Self-assessment ratings changed significantly following the study.

The calculated Chi-Square statistic was 72.43 with 4 degrees of freedom, corresponding to the five rating categories across two conditions (pre- and post-study). Referring to the Chi-Square distribution table, the critical value at the 0.0001 significance level for 4 degrees of freedom is 21.666. Since the computed value (72.43) far exceeds this threshold, the associated p-value is less than 0.0001.This result indicates a highly statistically significant difference in participants' self-assessment ratings before and after the simulation. Consequently, the null hypothesis of no association between the time of assessment and participants' rating levels is rejected, suggesting that the awareness program had a substantial impact on perceived cybersecurity knowledge.

DISCUSSION

The Chi-Square analysis revealed a statistically significant change in participants' self-assessed knowledge levels following the phishing simulation. Comparing expected values before and after the simulation, notable increases were observed in the 'Excellent' and 'Good' categories, while 'Poor' and 'Very Poor' ratings decreased. The total Chi-Square value of 72.43 demonstrates a marked improvement in participants' perceived cybersecurity awareness, suggesting that the simulation was effective in enhancing their confidence and understanding of phishing threats.The data highlights distinct patterns among the four schools. SST and SBMT, which recorded the highest phishing success rates, may require more targeted and frequent awareness interventions. This is crucial given that their staff may interact more frequently with financial systems, administrative communication, or have roles that make them high-value phishing targets. SAT and SET, though slightly less susceptible, also showed considerable vulnerability, which affirms the need for institution-wide awareness programs.

CONCLUSION

This study evaluated the effectiveness of phishing simulations as a cybersecurity awareness tool among staff of Federal Polytechnic Bali. The findings revealed a high initial level of vulnerability, with over two-thirds of participants engaging with the simulated phishing email, particularly those from the Schools of Science and Technology (SST) and Business and Management Technology (SBMT). However, the post-intervention results demonstrated a statistically significant improvement in staff self-assessed knowledge, with notable gains in the "Excellent" and "Good" categories. The Chi-Square Test confirmed that the observed differences were not by chance, underscoring the positive impact of targeted phishing

simulations in raising awareness and enhancing preparedness against social engineering threats.

The results highlight two key insights. First, academic institutions, like other sectors, are highly vulnerable to phishing attacks due to the diverse roles of staff, the large volume of sensitive data handled, and the growing sophistication of phishing tactics. Second, experiential learning through phishing simulations is an effective strategy for bridging awareness gaps, improving staff vigilance, and fostering confidence in handling suspicious messages. Nonetheless, gaps remain in proactive incident response, as some staff who identified the phishing attempt did not report it. This indicates the need for a stronger institutional culture of accountability and reporting to complement awareness programs.

RECOMMENDATIONS

Considering the findings from this study, several strategic actions are recommended to strengthen cybersecurity resilience and mitigate phishing threats within academic institutions:

1. Regular Phishing Simulations – Conduct routine, varied phishing exercises to strengthen staff readiness.
2. Cybersecurity Training – Integrate compulsory, updated training into staff development across all departments.
3. Reporting Mechanism – Establish a simple, centralized system for reporting phishing attempts to encourage vigilance.
4. Continuous Awareness – Sustain engagement through tips, posters, newsletters, and gamified learning activities.

By adopting these strategic recommendations, academic institutions can significantly reduce their exposure to phishing risks and build a robust human-centred defence mechanism to complement technological security infrastructure.

REFERENCE

1. Bach, M. P., Kamenjarska, T., &Žmuk, B. (2022). Targets of phishing attacks: The bigger fish to fry. *Procedia Computer Science*, *204*, 448-455.
2. Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., Lewinsmith, W., &Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers &Security*, *131*, 103313.

3. Bichnigauri, A., Kartvelishvili, I., Shonia, O., Bichnigauri, D., & Gudadze, O. (2024). STRENGTHENING CYBER DEFENSES-THE CRUCIAL ROLE OF PHISHING SIMULATION IN MODERN SECURITY STRATEGIES. *DEFENCE AND SCIENCE*.
4. Borgman, C. L. (2018). Open data, grey data, and stewardship: Universities at the privacy frontier. *Berkeley Technology Law Journal,* 33(2), 365–412.
5. Dolliver, D. S., Ghazi-Tehrani, A. K., & Poorman, K. T. (2021). Building a robust cyberthreat profile for institutions of higher education: An empirical analysis of external cyberattacks against a large university's computer network. *International Journal of Law, Crime, and Justice,* 66, Article 100484. https://doi.org/10.1016/j.ijlcj.2021.100484
6. Goel, S., Williams, K., &Dincelli, E. (2017). Got phished: Internet security and human vulnerability. *Journal of the Association for Information Systems,* 18(1), 22–44. https://doi.org/10.17705/1jais.00447
7. Iqbal, F., & Yusof, Z. B. (2024). Efficacy of Cybersecurity Awareness Training in Reducing Phishing Vulnerabilities in Organizations. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *8*(12), 10-21.
8. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, 564-74.
9. Li, W., Lee, J., Purl, J., Greitzer, F. L., Yousefi, B., & Laskey, K. B. (2020). Experimental investigation of demographic factors related to phishing susceptibility. In *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 2240–2249). https://doi.org/10.24251/HICSS.2020.274
10. Mercuri, D. (2025). Enhancing Cybersecurity Awareness: mitigating phishing risks for employees in a small company.
11. Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior*, *158*, 108274.
12. Phishing Attack Trends Report – 3Q 2023. (2023, November 13). Anti-Phishing Working Group.
13. Sharif, F. (2024, September). *Enhancing Cyber Security Resilience: Phishing Defense and the Importance of Measurement Strategies*.
14. Singar, A. V., & Akhilesh, K. B. (2020). Role of cyber-security in higher education. B. Akhilesh & P. F. Möller Dietmar (Eds.), *Smart Technologies: Scope and Applications* (pp. 249–264). Singapore: Springer.
15. Yeng, P. K., Fauzi, M. A., Yang, B., &Nimbe, P. (2022). *Investigation into phishing risk behavior among healthcare staff. Information*, 13(8), 392.