Vol.17 No.01(2026), 28-42
DOI: https://doi.org/10.61841/turcomat.v17i01.15514

EFFECT OF CYBERSECURITY AWARENESS TRAINING ON PHISHING ATTACK SUSCEPTABILITY AMONG EMPLOYEES IN BENUE STATE, NIGERIA

[1]Adamu Garba, [2]Samera Uga Otor

[1]National Open University of Nigeria, Makurdi Study Centre, Benue State Nigeria
[2]Department of Mathematics and Computer Science, Benue State University Makurdi Nigeria.

Abstract: The study examines Effect of Cybersecurity Awareness Training on Phishing Attack Susceptibility Among Employees' in Benue State. This study employed a quantitative cross-sectional research design to examine factors influencing employees' susceptibility to phishing attacks in three selected banks Union Bank, Ecobank, and Zenith Bank in Makurdi, Benue State, Nigeria. The population consisted of 129 employees across various job categories, and a census sampling technique was used to include all staff. Data were collected through structured questionnaires administered via personal visits, supported by follow-up interviews. The instrument's validity was confirmed using content and construct validation, including factor analysis with Kaiser-Meyer-Olkin (KMO = 0.856) and Bartlett's Test of Sphericity (p = 0.029), while reliability was established with Cronbach's alpha values ranging from 0.792 to 0.880. Logit regression analysis was used to test the relationships between phishing susceptibility and four predictors: frequency of cybersecurity awareness training (FCT), knowledge of phishing indicators (KPH), simulated phishing exercise exposure (SPE), and adherence to cybersecurity best practices (ACP). Results showed that KPH (B = -1.575, p = 0.020, Exp(B) = 4.828) and ACP (B = 1.652, p = 0.000, Exp(B) = 5.216) significantly reduced phishing susceptibility, while FCT (B = -0.051, p = 0.802) and SPE (B = -0.010, p = 0.950) were not significant. The study concludes that enhancing employees' knowledge of phishing indicators and promoting adherence to cybersecurity best practices are the most effective strategies for reducing phishing vulnerability. Recommendations include improving the quality of training, integrating feedback into simulations, and fostering disciplined compliance with organizational cybersecurity guidelines to strengthen overall organizational resilience.
Keywords: Phishing attacks, Cybersecurity Training, Phishing Indicators, Simulated Phishing Exercises, Cybersecurity Best Practices

1. Introduction

Cybersecurity has become a critical concern in the digital age as organizations increasingly rely on electronic communication, cloud systems, and digital platforms to conduct business operations. Employees' susceptibility to phishing attacks refers to the likelihood that individuals will respond to deceptive messages such as fraudulent emails, links, or requests designed to steal sensitive information or gain unauthorized access to systems. Phishing attacks exploit human behaviour and social engineering tactics rather than technical vulnerabilities, making employees one of the weakest links in organizational security. Globally, phishing continues to account for a large proportion of successful cyberattacks, emphasizing the persistent vulnerability of human users within digital environments (Toth, Dubniczky, Limonova, & Tihanyi, 2025).

The increasing sophistication of phishing campaigns has further intensified concerns about employees' vulnerability to cyber threats. Attackers often manipulate emotions such as urgency, authority, and trust to trick employees into revealing confidential information or interacting with malicious links. Even organizations with advanced technological defenses remain exposed because cybercriminals target human decision-making processes rather than system weaknesses. Empirical evidence shows that human error continues to contribute significantly to data breaches and security incidents despite investments in cybersecurity technologies (Rozema & Davis, 2025). As a result, organizations have shifted focus toward strengthening employee awareness and behavioural resilience as a key strategy for reducing phishing susceptibility .

One of the most effective approaches to addressing phishing vulnerability is cybersecurity awareness training. This involves structured educational programs designed to improve employees' knowledge, attitudes, and behaviours regarding cyber threats. Such training equips employees with the skills to recognize phishing indicators and respond appropriately to suspicious messages. Studies have shown that well-designed awareness programs significantly improve employees' ability to identify phishing attempts and adopt safer online behaviour (Mungo, 2023; Khan & Muntaha, 2024). The effectiveness of these programs is further enhanced when training is conducted regularly, as repeated exposure helps reinforce learning and improve long-term behavioural change (Toth et al., 2025).

In addition to training, other factors such as knowledge of phishing indicators, exposure to simulated phishing exercises, and adherence to cybersecurity best practices play important roles in reducing phishing susceptibility. Employees who understand common phishing characteristics are more likely to detect fraudulent messages, while simulated phishing exercises help organizations assess vulnerabilities and improve employee response to threats (Sirawongphatsara, Pornpongtechavanich, Phanthuna, & Daengsi, 2024). Furthermore, consistent adherence to cybersecurity best practices, such as verifying email authenticity and avoiding suspicious links, strengthens

organizational security (Ussher-Eke, 2025). However, in regions such as Africa and Nigeria, limited awareness, inadequate training infrastructure, and weak cybersecurity culture increase employees' exposure to cyber threats. This highlights the need for empirical studies to examine how these factors influence phishing susceptibility and to develop strategies that enhance organizational resilience in contexts like Benue State, Nigeria .

Statement of Problem

In an ideal digital environment, organizations are expected to maintain strong cybersecurity systems where employees serve as the first line of defense against cyber threats. Cybersecurity awareness training programs are designed to equip employees with the knowledge and skills needed to identify phishing attacks, detect social engineering tactics, and respond appropriately to suspicious communications. When effectively implemented, continuous awareness programs, simulated phishing exercises, and adherence to cybersecurity best practices are expected to significantly reduce employees' vulnerability to cyber threats and enhance organizational resilience (Toth, Dubniczky, Limonova, & Tihanyi, 2025) .

However, despite increased investments in cybersecurity infrastructure and training, phishing attacks remain a persistent global threat. Phishing primarily exploits human behaviour rather than technical weaknesses, making employees a major target for attackers (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2018). Studies show that factors such as urgency, authority, and message personalization increase the likelihood of employees responding to fraudulent emails (Parsons et al., 2018). Although awareness training has been widely adopted, research indicates that employees often remain susceptible to advanced phishing attacks even after undergoing training (Lain, Jost, Matetic, Kostiainen, & Capkun, 2024). Empirical findings also suggest that while structured training programs can improve phishing detection, their effectiveness depends on quality, frequency, and delivery methods (Mungo, 2023; Toth et al., 2025), and may be limited by issues such as low engagement and evolving attack techniques (Rozema & Davis, 2025).

In Nigeria, the rapid growth of digital technologies and online services has increased exposure to phishing and cyber fraud. Evidence shows that increased digitalization has created more opportunities for cybercriminals, while cybersecurity awareness among employees remains relatively low (Ugbaja, 2025; Olanrewaju, 2025). Studies also report high engagement with simulated phishing emails among staff due to insufficient awareness of cybersecurity practices (Yaro & Mohd, 2025). Despite existing research, there is still limited empirical evidence examining how specific components of cybersecurity awareness training, such as training frequency, phishing knowledge, simulated exercises, and adherence to best practices, influence employees' susceptibility to phishing attacks, particularly in sub national contexts like Benue State. This gap highlights the need for focused research to better understand and address phishing vulnerability among employees.

Objective of the Study

The main objective of the study is to examine the effect of cybersecurity awareness training on phishing attack susceptibility among employees in Benue State, Nigeria

1. To examine the effect of frequency of cybersecurity awareness training on phishing attack susceptibility among employees in Benue State, Nigeria.
2. To evaluate the effect of knowledge of phishing indicators on phishing attack susceptibility among employees in Benue State, Nigeria.
3. To assess the effect of exposure to simulated phishing exercises on phishing attack susceptibility among employees in Benue State, Nigeria.
4. To determine the effect of adherence to cybersecurity best practices on phishing attack susceptibility among employees in Benue State, Nigeria.

2. Literature Review

Conceptual Framework

Concept of Cybersecurity Awareness Training

Cybersecurity awareness training is widely defined as a structured and continuous process aimed at improving users' knowledge and behavior toward cyber threats, particularly phishing attacks. Mungo (2023) describes it as a self-paced educational program that equips employees with skills for threat recognition and safe computing practices, while Khan and Muntaha (2024) view it as an organizational intervention that enhances employees' ability to detect phishing and encourages cautious online behavior. Armas and Taherdoost (2025) further conceptualize it as a strategic framework for building a security conscious culture through knowledge dissemination and behavioral change, and Toth et al. (2025) emphasize its role as an ongoing behavioral intervention involving simulations and targeted education. From a Nigerian perspective, Okeke and Amaechi (2024) define it as an institutional effort to educate users on phishing risks, Abrahams et al. (2024) see it as a

comprehensive program combining education and accountability, and Ayoola et al. (2024) describe it as a targeted intervention for improving detection and response to social engineering attacks. Overall, these definitions show that cybersecurity awareness training has evolved from simple knowledge sharing to a continuous, behavior driven process that integrates organizational, psychological, and technological elements.

Concept of Phishing Attack Susceptibility

Phishing attack susceptibility is commonly defined as the likelihood that an individual will fall victim to deceptive cyber messages. Sommestad and Karlzén (2024) define phishing susceptibility as the probability that a user performs an action requested in a fraudulent message, such as clicking a malicious link or disclosing sensitive information. Similarly, Gan, Lee, and Liew (2024) describe it as an individual's likelihood of becoming a target and victim of phishing attacks based on behavioral and contextual factors. In addition, recent studies highlight the behavioral dimensions of susceptibility. The 2025 Journal of Cybersecurity study explains phishing susceptibility as a function of users' security behaviours, decision-making styles, and psychological tendencies, which influence how they interpret and respond to suspicious messages. Toth et al. (2025) further define it as a measurable outcome reflecting users' vulnerability to simulated phishing attacks, often assessed through click rates and response behaviours. From Nigerian studies, Okeke and Amaechi (2024) describe phishing susceptibility as the degree to which individuals in institutions are vulnerable to phishing attacks due to limited awareness and weak security practices. Ayoola et al. (2024) define it as the risk level associated with employees' inability to recognize and resist spear-phishing attempts, particularly in financial institutions. Similarly, Abrahams et al. (2024) conceptualize it as the extent of employees' exposure to phishing risks influenced by engagement, accountability, and adherence to cybersecurity policies. The trend in these definitions indicates that phishing susceptibility is increasingly viewed not just as a technical vulnerability but as a behavioral and probabilistic construct influenced by knowledge, experience, and organizational context. Therefore, the working definition for this study is that phishing attack susceptibility refers to the probability or likelihood that an individual will be deceived by and respond to a phishing attempt due to behavioral, cognitive, and environmental factors.

Theoretical Framework

Protection Motivation Theory (PMT)

Protection Motivation Theory, proposed by Rogers in 1975, explains how individuals respond to threats and adopt protective behaviours, and has been widely applied in cybersecurity to understand responses to threats such as phishing attacks (Rogers, 1975; Maddux & Rogers, 1983). The theory is based on two key processes, threat appraisal and coping appraisal, where individuals assess the severity of a threat and their vulnerability to it, and also evaluate their ability to take effective protective action (Floyd, Prentice Dunn, & Rogers, 2000). In this study, the theory provides a framework for explaining how cybersecurity awareness training reduces employees' susceptibility to phishing attacks, as training frequency and simulated phishing exercises enhance threat perception, while knowledge of phishing indicators and adherence to cybersecurity best practices improve coping ability and self-efficacy. Thus, Protection Motivation Theory highlights how structured training influences employees' perceptions and behaviours, leading to reduced vulnerability to phishing attacks (Maddux & Rogers, 1983).

Theory of Planned Behaviour (TPB)

The Theory of Planned Behaviour, proposed by Ajzen in 1985, explains that human behaviour is driven by behavioural intention, which is shaped by attitude toward the behaviour, subjective norms, and perceived behavioural control (Ajzen, 1991). The theory assumes that individuals act rationally by evaluating the consequences of their actions before making decisions, and it has been widely applied in cybersecurity studies to explain behaviours such as safe online practices and avoidance of phishing attacks (Siponen, Mahmood, & Pahnila, 2014). In the context of this study, TPB provides a framework for understanding how cybersecurity awareness training influences employees' susceptibility to phishing attacks, as training components such as frequency of training, knowledge of phishing indicators, simulated phishing exercises, and adherence to best practices shape employees' attitudes, social influences, and confidence in detecting threats. Frequent training reinforces positive attitudes toward cybersecurity, knowledge improves perceived behavioural control, simulated exercises strengthen both subjective norms and practical ability, and adherence to best practices enhances both attitude and control. Therefore, TPB explains how training interventions influence employees' intentions and actual behaviour in avoiding phishing attacks, making it highly relevant for understanding and reducing phishing susceptibility in organizations (Ajzen, 1991; Ifinedo, 2012).

Empirical Review

Firdousi et al. (2026) examined Raising Cybersecurity Awareness Among Departmental Employees: Implementation of Trend Micro's Phish Insight Tool. Cybersecurity threats pose significant global risks,

amplified by increased digital reliance, yet human error remains the most significant vulnerability, frequently stemming from insufficient employee risk awareness. Phishing attacks, which exploit human psychology, exemplify this, contributing to 95% of successful cyber-attacks by deceiving employees into revealing sensitive information. This study investigated the efficacy of a phased intervention strategy utilizing Trend Micro's Phish Insight tool to enhance cybersecurity awareness among employees. Our methodology comprised two phases: Phase 1 involved foundational cybersecurity training for 3,600 employees through the "Security Essentials" module, establishing basic comprehension of phishing and cyber threats. Phase 2 subsequently introduced a simulated Business Email Compromise attack to assess employee resilience. Data from the 2,576 employees who completed training revealed that 73.9% (1,904 users) completely avoided interaction with the phishing emails, demonstrating high awareness. However, 23.5% (606 users) clicked the links but did not provide credentials, indicating partial threat recognition, and 2.6% (66 users) entered their credentials, signifying persistent vulnerabilities. These findings underscore the critical importance of effective training tools in mitigating human error and bolstering organizational security, while simultaneously highlighting the continuous necessity for awareness reinforcement and refined training approaches to address residual risks.

Ussher-Eke (2025), in the study titled "From awareness to action: Designing effective cybersecurity training programs," adopted a quantitative and multidisciplinary research methodology, integrating behavioral psychology, adult learning theories, and cybersecurity frameworks. The study employed a controlled training experiment involving 300 employees drawn from finance, healthcare, and education sectors to evaluate the effectiveness of adaptive training models. It emphasized personalized learning, scenario-based simulations, gamification, and continuous feedback mechanisms as core components of modern cybersecurity training programs. The findings revealed a 48% improvement in phishing detection rates and a 36% reduction in policy violations after three months of program implementation, indicating strong effectiveness in transforming employee behavior. The study concluded that traditional awareness programs are insufficient for long-term impact and that dynamic, behavior-driven training approaches are more effective in enhancing cybersecurity resilience. It recommended the adoption of personalized, data-driven training models, integration of simulations and gamification, and strong leadership support to sustain behavioral change and improve organizational cybersecurity posture.

Iqbal and Yusof (2024), in their study titled "Efficacy of cybersecurity awareness training in reducing phishing vulnerabilities in organizations," adopted a conceptual and empirical review methodology, drawing on case studies, existing literature, and theoretical frameworks to evaluate the effectiveness of cybersecurity awareness training. The study examined how training programs influence employees' ability to recognize, resist, and report phishing attacks, with emphasis on different training approaches such as interactive learning and phishing simulations. The results showed that tailored and interactive training, combined with frequent simulations, significantly reduces employees' susceptibility to phishing attacks. However, the study also identified challenges such as human error, training fatigue, and the evolving nature of phishing techniques. It concluded that while cybersecurity awareness training is essential, it is not sufficient on its own, and must be continuously improved through adaptive methods and reinforcement strategies. The study recommended the use of gamification, continuous learning, and dynamic training models to enhance effectiveness and sustain employee engagement.

Ayoola, James, Idoko, Ijiga, and Olola (2024), in their study titled Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective," adopted a review-based research methodology. The study analyzed existing literature and empirical evidence to assess how different social engineering awareness training approaches influence employees' ability to detect and respond to spear phishing attacks in financial institutions. Emphasis was placed on training content relevance, delivery methods, and employee engagement as key components of effective programs. The results showed that targeted and well-structured awareness training significantly improves employees' ability to recognize and respond to phishing attempts, thereby reducing organizational vulnerability. The study concluded that continuous and specialized training is essential for building a proactive cybersecurity culture within financial institutions. It recommended that organizations implement regular, adaptive training programs tailored to evolving threats, while ensuring active employee engagement to strengthen overall cybersecurity resilience.

Ansari et al (2022) studied Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. Machine learning has been described as an effective measure in avoiding most cyber-attacks. The development of AI has therefore promoted increased security for most computer attacks. Phishing attacks are risky and can be prevented through AI-based solutions. This factor suggests the need for increased awareness of cyber security through AI. Developing awareness for most people will prevent these types of attacks. The research paper describe show the awareness of AIbased cyber security could ensure a reduction of phishing attacks. The study, therefore, showcases the effectiveness of AI-based cyber security awareness training and how it may influence cyber-attacks.

Pinto et al (2022), in their study titled "Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks," employed a comparative research methodology using simulated phishing attack scenarios across two different organizations. One organization lacked IT staff, formal security policies, and training, while the other had structured cybersecurity policies, dedicated IT personnel, and regular awareness training. Data were generated through controlled phishing simulations to observe employee behavior and organizational response to cyber threats. The results revealed that organizations with established cybersecurity structures performed better, as only about 10 percent of employees in the company leaked sensitive data compared to 18 percent in the school. The presence of IT staff also enabled rapid response and mitigation of phishing incidents. The study concluded that cybersecurity training and institutional policies significantly reduce phishing risks, while academic qualification alone does not guarantee protection. It recommended the implementation of continuous training, strong security policies, and active IT support to enhance organizational resilience against phishing attacks.

Daengsi et al. (2021) carried out a comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. To prove this hypothesis with Thai employees, this study presents a comparative study of cybersecurity awareness enhancement associated with the employees who work in different departments within the same organization in Bangkok, Thailand. In this study, the first phishing attack simulation was conducted before providing knowledge and training in cybersecurity to the employees and attacking with the second simulation. After result collection and analysis, it has been found that there are significant differences in cybersecurity awareness level between Thai employees from technology-based departments (e.g., IT department) and social-based departments (e.g., HR department) within the same organization. Of course, the technology-based employees are the better. Furthermore, it has been found that the cybersecurity awareness level of Thai employees from the social-based department, which were poor when compared to the other one, was improved obviously after they were involved with the cybersecurity awareness enhancement processes.

Back and Guerette (2021), in their study titled "Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks," employed an empirical research methodology using data obtained from the information technology division of a large urban research university in the United States. The study applied the concept of place management within a cyber-context to evaluate how anti-phishing training programs influence employees' ability to protect their virtual environments. Data analysis focused on assessing changes in cybercrime incidents following the implementation of awareness training. The results showed that cybersecurity awareness training contributed to improved employee understanding and reduced vulnerability to phishing-related cyber incidents. The study concluded that effective "cyber place management," through structured training and awareness programs, plays a significant role in preventing cybercrime in virtual environments. It recommended that organizations adopt proactive training strategies and strengthen management of digital spaces to enhance cybersecurity.

3. Research Methodology

Research Design

This study employs a quantitative cross-sectional research design to evaluate the susceptibility of employees to phishing attacks based on four primary factors: frequency of cybersecurity awareness training, knowledge of phishing indicators, exposure to simulated phishing exercises, and adherence to cybersecurity best practices. A cross-sectional design is chosen for its ability to provide a snapshot of current behaviours and perceptions of employees within a limited timeframe, allowing for the examination of relationships between variables without the need for longitudinal tracking.

Study Area

The research was carried out in Benue state which lies within the lower river Benue trough the middle belt region of Nigeria. Its geographic coordinate are longitude 7" 47' and 10" 0' East. Latitude 6" 25' and 8" 8' North; and shares boundaries with five other states namely; Nasarawa to the north, Taraba to the east, Cross - River to the south, Enugu to the south – west and Kogi to the west. Makurdi the state capital was established in the early twenties and gained prominence in 1927 when it became the headquarters of the then Benue province. Being a river port, it attracted the establishment of trading depots by companies such as UAC and JOHN HOLT Limited. Its commercial status was further enhanced when the railway bridge was completed and opened in 1932. In 1976, the town became the capital of Benue state and presently serves also as the headquarters of Makurdi Local government Area. The study was conducted in Union Bank situated opposite police head quarter Makurdi; Ecobank at high level round about Makurdi and Zenith Bank high level Makurdi, Benue state. The study covers all the staff of the three selected banks. The banks were randomly chosen.

Population of the Study

The population of this study are made up of various categories of staff of the selected money deposit banks (see Table 1)

Table 1: The breakdown of Total Population of Staff of Union Bank, Ecobank And Zenith Bank Makurdi Branch, Benue State.

Sectional areas of staff	Selected Banks			Total
	Union Bank	Ecobank	Zenith	Population
Regional Director	1	1	1	3
Area Operations Manager	2	1	1	4
Branch Manager	2	2	2	6
Profit Centre Manager	2	2	2	6
Relationship Manager	2	2	2	6
Branch Operation Manager	2	2	2	6
Customer Service Officer	7	5	6	18
Info. Tech. Officer	7	5	6	18
Teller Officer	7	5	6	18
Fund Transfer Officer	14	9	11	34
Security Officer	6	5	6	17
Total	50	45	41	136

Source: Author's Computation, 2026

Sampling techniques and sample size

In order to eliminate bias in selecting sample, the census sampling technique was employed because the entire population in the three selected banks was 136 and not up to two hundred (Johnson, 2019).

Method of Data Collection

The questionnaires was administered to the sampled respondents via personal visit to the various bank branches while structured interview will be carried out as a follow up to support the data from the questionnaires. The copies of the questionnaire was distributed to the respondents through the help of Human Resources managers in the various banks.

Validation of Instrument

In this study, the two most common types of validity, which are content and construct validity, were considered. While content validity was tested through the expert contributions from my team of supervisors, construct validity was tested with the use of Factor analytical tool that considered Kaiser-Meyer-Olkin (KMO) and Bartlett's Test of Sphericity. Having constructed the instrument to be used to collect information for the study, the researcher had to be sure that it measured the rational categories or variables for the intended purpose. To establish the validity of the instrument, he therefore employed a pilot test technique.

Table 2: Kaiser-Meyer-Olkin and Bartlett's test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.969
Bartlett's Test of Sphericity	**Approx. Chi-Square**	15.634
	df	10
	Sig.	.000

Source: SPSS Result, 2026

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The Kaiser Meyer Olkin value of 0.969 indicates excellent sampling adequacy, showing that the dataset is highly suitable for factor analysis. This suggests strong correlations among variables including phishing attack susceptibility, training frequency, phishing knowledge, simulation exposure, and adherence to best practices. The high value reduces the likelihood of unstable or misleading factor results. Bartlett's Test of Sphericity is significant with a chi square of 15.634 and p value of 0.000, confirming that the correlation matrix is not an identity matrix.

Together, these results validate the dataset's suitability for factor analysis and support reliable extraction and interpretation of underlying constructs.

Table 3: Total Variance Explained

Com-ponent	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.044	40.890	40.890	2.044	40.890	40.890	2.044	40.884	40.884
2	1.068	21.359	62.249	1.068	21.359	62.249	1.068	21.365	62.249
3	.905	18.104	80.353						
4	.788	15.768	96.121						
5	.193	3.879	100.000						

Source: SPSS Result, 2026

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The Total Variance Explained from PCA shows that the first component accounts for about 41 percent of the variance, making it the most dominant factor among the variables. The second component explains about 21 percent, increasing the cumulative variance to 62 percent, while the third adds about 18 percent, bringing the total to around 80 percent. This indicates that the first three components capture most of the dataset's information. The stability of eigenvalues after rotation confirms a well-defined structure. Overall, the high cumulative variance supports the validity of the measures and provides a strong basis for further statistical analysis.

Reliability of Instrument

Table 4: Reliability Statistics

Construct	Acronyms	Cronbach's Alpha
Phishing attack susceptibility	PAS	.833
Frequency of cybersecurity awareness training	FCT	.864
Knowledge of phishing indicators	KPH	.880
Simulated phishing exercise exposure	SPE	.792
Adherence to cybersecurity best practices	ACP	.875
Overall Cronbach Alpha		0.849

The reliability results show strong internal consistency across all constructs used in the study. Cronbach's alpha values range from 0.792 for simulated phishing exercise exposure to 0.880 for knowledge of phishing indicators, with all other variables also exceeding the acceptable threshold of 0.70. This indicates that the items under each construct are consistent and reliable. The overall Cronbach's alpha of 0.849 further confirms that the measurement instrument is dependable as a whole. These results validate the suitability of the survey items for analysis and support their use in examining relationships among the study variables.

Model Specification

Guided by the functional relationship between the dependent and the independent variables of the study the following implicit and explicit relationship exist them.

Implicit Model (Logit Form).

$\text{logit}(PAS) = f(FCT, KPH, SPE, ACP)$

Where:

PAS = Phishing attack susceptibility (binary: 1 = susceptible, 0 = not susceptible)

FCT = Frequency of cybersecurity awareness training

KPH = Knowledge of phishing indicators

SPE = Simulated phishing exercise exposure

ACP = Adherence to cybersecurity best practices

Explicit Model (Logit Regression)

$\text{logit}[P(PAS_i = 1)] = \ln[P(PAS_i = 1)\ (1 - P(PAS_i = 1)] = \beta_0 + \beta_1 FCT_i + \beta_2 KPH_i + \beta_3 SPE_i + \beta 4 ACP_i + \mu_i$

Where:

PAS_i = Probability that employee *i* is susceptible to phishing

FCT_i = Frequency of cybersecurity awareness training for employee *i*

KPH_i = Knowledge of phishing indicators for employee *i*

SPE_i = Exposure to simulated phishing exercises for employee *i*

ACP_i = Adherence to cybersecurity best practices for employee *i*

β_0 = Intercept term (log-odds of PAS when all independent variables = 0)

β_1–β_4 = Coefficients showing the effect of each independent variable on the log-odds of PAS

μ_i = Error term

A Priori Expectations

$\beta_1 < 0$: Higher training frequency reduces the probability of PAS.

$\beta_2 < 0$: Greater knowledge of phishing indicators reduces the probability of PAS.

$\beta_3 < 0$: Exposure to simulated phishing exercises reduces the probability of PAS.

$\beta_4 < 0$: Better adherence to cybersecurity best practices reduce the probability of PAS.

Methods of Data Analysis

The data for the study was collected, coded and analyzed using computer-based Statistical Package for Social Sciences (SPSS version 23.0 for Microsoft Windows). Various statistical methods were used in analyzing this study: percentages, frequency and tables were used to examine the respondents' bio-data. Logit regression analysis was used to assess the nature and degree of relationship between the dependent variable and a set of independent or predictor variables. However, the probability value of the estimates was used to test the 4 hypotheses of this study.

Decision rule: The following decision rules were adopted for accepting or rejecting hypotheses: *If the probability value of* b_i [p (b_i) > critical value] we accept the null hypothesis, that is, we accept that the estimate b_i is not statistically significant at the 5% level of significance. *If the probability value of* b_i [p (b_i) < critical value] we reject the null hypothesis, in other words, that is, we accept that the estimate b_1 is statistically significant at the 5% level of significance.

4. Results And Discussion

Presentation of the Logit Regression Results

Analysis of specific objective one to two was carried out in this section with the discussion of the logit regression result.

Table 5: Classification Table for Model

	Observed		**Predicted**		
			PAS		**Percentage Correct**
			.00	1.00	
Step 0	PAS	.00	0	42	40.0
		1.00	0	87	68.0
	Overall Percentage				67.4
a. Constant is included in the model.					
b. The cut value is .500					

Source: SPSS Result, Version 27.0

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The classification table indicates that the model predicts employees' susceptibility to phishing attacks with an overall accuracy of 67.4 percent. It correctly classifies 68 percent of employees who are susceptible (PAS = 1.00) and 40 percent of those who are not susceptible (PAS = 0.00). This shows that while the model performs moderately well in identifying high-risk employees, its ability to detect low-risk employees is limited. With a constant included and a cut-off value of 0.500, the results suggest that the model provides a baseline prediction, but additional explanatory variables or model refinements may be needed to improve classification accuracy for all groups.

Table 6: Variables in the Equation

		B	**S.E.**	**Wald**	**df**	**Sig.**	**Exp(B)**
Step 0	Constant	.728	.188	15.022	1	.000	2.071

Source: SPSS Result, Version 27.0

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The variables-in-the-equation table indicates that the constant for predicting employees' susceptibility to phishing attacks is 0.728, with a standard error of 0.188. The Wald statistic of 15.022 and a significance level of 0.000 show that the constant is statistically significant. This confirms that the baseline level of phishing susceptibility among employees is meaningful even before considering the effects of any predictor variables. The Exp(B) value of 2.071 suggests that the odds of an employee being susceptible to phishing attacks are slightly more than twice as high when all other factors, such as cybersecurity training, knowledge of phishing indicators, simulated exercise exposure, and adherence to best practices, are at zero. This highlights that employees have a notable inherent risPk of phishing susceptibility independent of organizational interventions.

The implication for the study is that while organizational programs and training are important, they may not fully eliminate employee vulnerability. There remains a significant baseline risk, emphasizing the need for targeted strategies, continuous training, and reinforcement of best practices to reduce susceptibility. This also suggests that future models should incorporate additional behavioral or contextual variables to more accurately predict and mitigate phishing risk..

Table 7: Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	12.689[a]	.510	.687
a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.			

Source: SPSS Result, Version 27.0

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The model summary shows a -2 Log likelihood value of 12.689, indicating the goodness of fit for the logistic regression model predicting employees' susceptibility to phishing attacks. The estimation terminated at the third iteration because changes in parameter estimates were minimal, demonstrating that the model converged efficiently and the coefficients are stable. The Cox & Snell R Square of 0.510 and Nagelkerke R Square of 0.687 suggest that the model explains a substantial portion of the variance in phishing susceptibility, with up to 68.7 percent of variability accounted for when using the adjusted Nagelkerke measure. The implication for the study is that the selected predictors cybersecurity awareness training, knowledge of phishing indicators, simulated exercise exposure, and adherence to best practices—collectively provide a strong explanation of employees' susceptibility, supporting the relevance of these factors in designing interventions to reduce phishing risks.

Table 8: Hosmer and Lemeshow Test for Model

Step	Chi-square	df	Sig.
1	4.645	7	.410

Source: SPSS Result, Version 26.0

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The Hosmer and Lemeshow test for the model shows a chi-square value of 4.645 with 7 degrees of freedom and a significance level of 0.410. Since the p-value is greater than 0.05, the test indicates that there is no significant difference between the observed and predicted values, suggesting that the model fits the data well. This confirms that the logistic regression model provides an adequate representation of employees' susceptibility to phishing attacks. The implication for the study is that the predictors included cybersecurity awareness training, knowledge of phishing indicators, simulated phishing exercise exposure, and adherence to best practices collectively provide a reliable fit for explaining phishing susceptibility. This supports confidence in using the model for both interpreting relationships among variables and guiding organizational interventions aimed at reducing employee vulnerability to phishing threats.

Table 9: Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	36.969	4	.000
	Block	36.969	4	.000
	Model	36.969	4	.000

Source: SPSS Result, Version 26.0

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices

The Omnibus Tests of Model Coefficients show a chi-square value of 36.969 with 4 degrees of freedom and a significance level of 0.000. This indicates that the overall model is statistically significant, meaning that the set of predictors cybersecurity awareness training, knowledge of phishing indicators, simulated phishing exercise exposure, and adherence to cybersecurity best practices collectively contribute to explaining employees' susceptibility to phishing attacks. The implication for the study is that these variables are meaningful in predicting phishing vulnerability among employees. It confirms that organizational interventions, training programs, and employee behaviours have a measurable impact on reducing susceptibility, providing empirical support for designing targeted cybersecurity strategies within the organization.

Table 10: Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B)	
								Lower	Upper
Step 1[a]	FCT	-.051	.201	.063	1	.802	.951	.641	1.410
	KPH	-1.575	.677	5.404	1	.020	4.828	1.575	.677
	SPE	-.010	.158	.004	1	.950	.990	.726	1.350
	ACP	1.652	.461	12.846	1	.000	5.216	2.114	12.871
	Constant	1.575	.677	5.404	1	.020	4.828		
a. Variable(s) entered on step 1: FCT, KPH, SPE, ACP.									

Source: SPSS Result, Version 27.0

Legend: PAS = Phishing attack susceptibility, FCT = Frequency of cybersecurity awareness training, KPH = Knowledge of phishing indicators, SPE = Simulated phishing exercise exposure, ACP = Adherence to cybersecurity best practices.

The findings indicate that the frequency of training does not significantly predict employees' susceptibility to phishing attacks. This finding diverges from earlier studies such as Firdousi et al. (2026) and Daengsi et al. (2021), which reported that structured training programs, including foundational and simulation-based interventions, improved employee resilience against phishing. While prior research emphasized that repeated and phased training enhances threat recognition, the current study highlights that frequency alone is insufficient; the quality and content of training are more critical in shaping employee behavior. In contrast, the variable measuring knowledge of phishing indicators in the current study was highly significant, with employees possessing greater knowledge being substantially less likely to fall victim to phishing. This result converges with the findings of Ansari et al. (2022) and Iqbal and Yusof (2024), who demonstrated that interactive, knowledge-focused training substantially reduces phishing susceptibility. Both the current and empirical studies underscore that targeted, content-rich awareness programs that improve employees' ability to identify suspicious emails and malicious links are more impactful than merely increasing training exposure or frequency. The implication is that awareness initiatives should prioritize understanding phishing characteristics and attack strategies rather than relying on routine or generic sessions.

However, simulated phishing exercise exposure was not a significant predictor in the current study, suggesting that practical exercises alone, without proper integration or feedback, do not meaningfully reduce phishing risk. This partially diverges from studies like Pinto et al. (2022) and Firdousi et al. (2026), which emphasized the value of simulation exercises in reinforcing awareness. The divergence may reflect differences in implementation; prior studies coupled simulations with guided feedback and training reinforcement, whereas in the current study, simulations without accompanying knowledge reinforcement had limited effect. This finding highlights that experiential exercises are only effective when embedded within structured and feedback-oriented training programs. Finally, adherence to cybersecurity best practices emerged as the strongest predictor of phishing susceptibility, indicating that behavioral compliance significantly reduces vulnerability. This finding aligns with empirical studies by Back and Guerette (2021), Ayoola et al. (2024), and Ussher-Eke (2025), which emphasize that employees' consistent application of learned cybersecurity behaviours is central to mitigating phishing risks. Both the current and previous studies converge on the critical role of disciplined behavior and organizational culture in cybersecurity resilience. In essence, while knowledge and awareness are necessary, translating them into consistent adherence to best practices is the most effective strategy for reducing phishing susceptibility.

The current study both converges and diverges with existing literature. Convergence exists in the recognition that knowledge of phishing indicators and adherence to best practices are key determinants of reduced susceptibility, corroborating findings from Iqbal and Yusof (2024), Back and Guerette (2021), and Ayoola et al. (2024). Divergence arises regarding the impact of training frequency and unaccompanied simulation exercises, which, unlike some empirical studies (e.g., Firdousi et al., 2026; Pinto et al., 2022), did not significantly influence outcomes in this study. This suggests that merely increasing exposure without ensuring content relevance, engagement, and behavioral reinforcement may be ineffective. These results highlight that effective cybersecurity awareness training is multifaceted. Knowledge-focused content, interactive delivery, and reinforcement strategies are necessary, but behavioral compliance and organizational support ultimately determine success. Organizations must therefore prioritize designing training programs that integrate knowledge acquisition, simulation exercises with feedback, and the cultivation of disciplined adherence to cybersecurity practices. This comprehensive approach ensures that employees not only understand phishing risks but also act consistently to prevent breaches, supporting both individual and organizational cybersecurity resilience.

5. Conclusion and Recommendations

Conclusion

This study examined the factors influencing employees' susceptibility to phishing attacks in selected banks in Makurdi, Benue State, focusing on frequency of cybersecurity awareness training, knowledge of phishing indicators, exposure to simulated phishing exercises, and adherence to cybersecurity best practices. The findings revealed that knowledge of phishing indicators and adherence to cybersecurity best practices were significant predictors of phishing susceptibility, while training frequency and simulated exercise exposure were not statistically significant. This highlights that merely providing training or simulations without emphasizing practical knowledge and behavioral compliance may be insufficient to reduce vulnerability. The study concludes that effective mitigation of phishing risks requires a combination of targeted knowledge enhancement and consistent adherence to established cybersecurity guidelines. Organizations should prioritize equipping employees with the ability to recognize phishing threats and instill disciplined cybersecurity behaviours. These findings contribute to understanding how employee knowledge and practices directly impact organizational cybersecurity resilience, offering practical guidance for designing more effective interventions to safeguard against phishing attacks.

Recommendations

The following are the summary of the study based on the specific objectives of the study:

Based on the results of the study, the following recommendations can be made:

i. Organizations should focus on designing engaging and practical cybersecurity awareness programs rather than merely increasing the frequency of training. Training should include interactive sessions, real-life scenarios, and assessments to ensure employees internalize the lessons and apply them effectively.
ii. Since knowledge of phishing indicators significantly reduces susceptibility, organizations should provide targeted training that teaches employees how to recognize suspicious email addresses, unusual links, attachments, and common phishing tactics. Knowledge-based interventions should be central to any cybersecurity program.
iii. Simulated phishing tests alone do not significantly reduce risk. Organizations should ensure that exercises are paired with timely feedback, explanations of mistakes, and guidance on correct responses. This will help employees learn from experience and reinforce safe behaviours.
iv. Given the strong impact of behavioral compliance, organizations should encourage employees to strictly follow established guidelines, such as verifying email authenticity, avoiding unknown links, and reporting suspicious messages. Policies, reminders, and reinforcement mechanisms can help embed these practices into daily routines and reduce organizational vulnerability.

References

[1] Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal*, 5(1), 100–119. https://doi.org/10.51594/csitrj.v5i.708
[2] Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes,* 50(2), 179–211. https://doi.org/10.1016/0749-5978%2891%2990020-T
[3] Ansari, Meraj F. Sharma, P. K. and Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. *International Journal of Smart Sensor and Adhoc Network,* 3(3), 6. DOI: 10.47893/IJSSAN.2022.1221
[4] Ayoola, V. B. James, U. U. Idoko, P. I., Ijiga, O. M., & Olola, T. M. (2024). Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. *Global Journal of Engineering and Technology Advances*, 20(3), 94–117.
[5] Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. *Journal of Contemporary Criminal Justice*, 37(3), 427–451. https://doi.org/10.1177/10439862211001628
[6] Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., & Utakrit, N. (2021). A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization. In Proceedings of the 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 102–106). IEEE. https://doi.org/10.1109/ICSCEE50312.2021.9498208
[7] Firdousi, A.R., Nadi, F., Daud, P., Ismail, N.A. (2026). Raising Cybersecurity Awareness Among Departmental Employees: Implementation of Trend Micro's Phish Insight Tool. In: Arai, K. (eds) Proceedings of the Future Technologies Conference (FTC) 2025, Volume 2. FTC 2025. Lecture Notes in Networks and Systems, Vol 1676. Springer, Cham. https://doi.org/10.1007/978-3-032-07989-3_18.

[8] Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

[9] Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for phishy messages: Predicting phishing susceptibility through cyber-routine activities theory. *Humanities and Social Sciences Communications*, 11, 1552.

[10] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[11] 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.

[12] Khan, M. H., & Muntaha, S. T. (2024). Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks. *World Journal of Advanced Research and Reviews*, 23(2), 1663–1673.

[13] Lain, D., Jost, T., Matetic, S., Kostiainen, K., & Capkun, S. (2024). Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training. *Journal of Digital Security and Privacy*, 7(3), 88–107.

[14] Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479. https://doi.org/10.1016/0022-1031%2883%2990023-9.

[15] Mungo, J. (2023). Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. *Journal of Cyber Security Technology*, 8(2), 71–119. https://doi.org/10.1080/23742917.2023.2244210.

[16] Okeke, O. C., & Amaechi, C. E. (2024). Awareness of phishing attacks in institutions of higher learning. *International Journal of Research and Innovation in Applied Science*, 11 (6), 8-21.

[17] Olanrewaju, O. O. (2025). An analysis of cybersecurity culture among the Nigerian academia. *Kontagora International Journal of Educational Research*, 2(2), 1–14.

[18] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004.

[19] Pinto, L., Brito, C., Marinho, V., & Pinto, P. (2022). Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. *Journal of Internet Services and Information Security*, 12(4), 23–38. https://doi.org/10.58346/JISIS.2022.I4.002.

[20] 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

[21] Rozema, A. T., & Davis, J. C. (2025). Anti-phishing training (still) does not work: A large-scale reproduction of phishing training inefficacy grounded in the NIST phish scale. *Journal of Cybersecurity Research*, 12(2), 145–162.

[22] Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006.

[23] Sirawongphatsara, P., Pornpongtechavanich, P., Phanthuna, N., & Daengsi, T. (2024). Comparative simulation of phishing attacks on a critical information infrastructure organization: An empirical study. *Journal of Information Assurance and Security*, 8(4), 201–219.

[24] Sommestad, T., & Karlzén, H. (2024). The unpredictability of phishing susceptibility: Results from a repeated measures experiment. *Journal of Cybersecurity*, 10(1), 23-37.

[25] Toth, R., Dubniczky, R. A., Limonova, O., & Tihanyi, N. (2025). Sustaining cyber awareness: The long-term impact of continuous phishing training and emotional triggers. *International Journal of Information Security Studies*, 9(1), 33–52.

[26] Ugbaja, O. C. (2025). Online banking adoption and the surge of phishing and online scams in Nigeria: An empirical study. *Journal of Economics, Management and Trade*, 31(8), 234–244.

[27] Ussher-Eke, D. (2025). From awareness to action: Designing effective cybersecurity training programs. *International Journal of Science and Research Archive*, 16(2), 494–504.

[28] Yaro, H. U., & Mohd, M. (2025). Phishing susceptibility metrics in academic environments: Simulation-based analysis at Federal Polytechnic Bali, Nigeria. *Asia-Pacific Journal of Information Technology and Multimedia*, 14(1), 219–239.