IMPACT OF PHISHING AND SOCIAL ENGINEERING ATTACKS ON DIGITAL FINANCIAL SERVICES IN NIGERIA

[1]Success Ikechi Kanu [2]Uzochukwu Ezekwere [3]Uzoma Donatus Okwara

[1]Department of Finance, School of Post Graduate Studies. Kingsley Ozumba (KO) Mbadiwe University, Ideato Imo State, Nigeria.
[2]Department of Accounting Kingsley Ozumba Mbadiwe University, Ideato Imo state, Nigeria.
[3]Directorate of General Studies, Philosophy Unit, Federal University of Technology Owerri Imo State.

Abstract

The increasing adoption of digital financial services in Nigeria has heightened concerns about phishing and social engineering attacks, which pose significant risks to users and the wider digital financial ecosystem. This study examined the influence of cybersecurity awareness, digital competence, and security behavior on users' exposure and susceptibility to phishing and social engineering attacks in Nigeria's digital financial services sector. Primary data were collected using a structured questionnaire and analyzed through Cronbach's Alpha, Pearson Product Moment Correlation, and Multiple Regression techniques. The reliability analysis showed acceptable internal consistency across the study constructs, with security behavior recording the highest reliability. Correlation results revealed a weak but statistically significant positive relationship between cybersecurity awareness and users' exposure and susceptibility to attacks ($r = 0.131$, $p = 0.049$). Digital competence showed a weak positive but statistically insignificant relationship ($r = 0.123$, $p = 0.066$), while security behavior demonstrated the strongest weak positive and statistically significant relationship ($r = 0.178$, $p = 0.007$). Multiple regression analysis indicated that the three predictors jointly had a statistically significant influence on users' exposure and susceptibility ($F = 3.084$, $p = 0.028$). However, the model explained only 4% of the variance ($R^2 = 0.040$), suggesting that other behavioral, technological, and contextual factors contribute to vulnerability. The study recommends strengthening cybersecurity awareness, practical digital security education, safe online practices, and complementary institutional and technological safeguards to reduce users' vulnerability and improve the security of Nigeria's digital financial services ecosystem.

Key words: *Cybersecurity awareness, digital competence, security behavior, cyber threats, digital safety, Nigeria.*

Introduction

The use of digital financial services has increased significantly in Nigeria over the past few years. More people now carry out financial transactions through mobile banking applications, fintech platforms, and agent banking services. These innovations have made banking easier and more accessible, especially for people who previously had little or no access to formal financial services. Reports from the National Bureau of Statistics show that mobile money transactions reached about ₦18.6 trillion in 2023, reflecting the growing acceptance of digital financial services in the country (NBS, 2023).

Despite these benefits, the increasing use of digital platforms has also created new security challenges. As more people rely on online financial services, cybercriminals have developed different methods of exploiting unsuspecting users. Two of the most common methods are phishing and social engineering attacks. These attacks involve tricking individuals into revealing sensitive information such as passwords, account details, PINs, and other confidential data (Mitnick & Simon, 2011; Hadnagy, 2018).

Unlike some cyberattacks that target weaknesses in computer systems, phishing and social engineering attacks mainly take advantage of human mistakes. Cybercriminals often use fake messages, emails, phone calls, or websites to deceive people into providing personal information. Because these attacks rely on manipulation rather than technical hacking, they can be difficult to detect and prevent. As the use of digital technology continues to expand, the methods used by fraudsters are also becoming more advanced and convincing (Verizon, 2024).

Trust is very important in any financial system. People are more willing to use digital financial services when they believe their money and personal information are safe. However, the increasing number of online scams and fraudulent activities can reduce users' confidence in these services. This situation may discourage people from fully embracing digital financial platforms. It is therefore important to understand the factors that make individuals vulnerable to phishing and social engineering attacks. Against this background, this study examines how awareness, digital literacy, and security practices influence users' susceptibility to these forms of cyber fraud.

Statement of the Problem

The rapid expansion of digital financial services has transformed financial transactions in Nigeria by improving accessibility, convenience, and financial inclusion. However, this digital transformation has also created new opportunities for cybercriminals, particularly through phishing and social engineering attacks that exploit users rather than technological systems. These attacks manipulate individuals into revealing passwords, one-time passwords (OTPs), account credentials, and other sensitive financial information, making them one of the most persistent threats to the security of

digital financial services. Recent cybersecurity reports by the Nigeria Inter-Bank Settlement System (NIBSS, 2024), the Central Bank of Nigeria (CBN, 2024), and the Verizon Data Breach Investigations Report (2024) indicate that phishing and social engineering remain among the leading techniques used to compromise users' accounts and facilitate electronic payment fraud.

Despite sustained investments by banks, fintech firms, and regulatory authorities in cybersecurity technologies, electronic payment fraud has continued to increase in Nigeria. According to NIBSS (2024), financial losses arising from electronic payment fraud increased from ₦2.96 billion in 2019 to ₦17.67 billion in 2023 and rose sharply to ₦52.26 billion in 2024. While these figures represent overall electronic payment fraud, recent industry reports attribute a substantial proportion of successful fraud incidents to phishing and social engineering attacks, which exploit human judgement rather than technical weaknesses. This trend suggests that technological security measures alone are insufficient to mitigate cyber fraud if users remain susceptible to deception and manipulation.

Existing studies on digital financial security have predominantly focused on technological safeguards, cybersecurity infrastructure, encryption techniques, and institutional fraud prevention mechanisms. Comparatively less empirical attention has been devoted to the human and behavioural factors that influence users' exposure and susceptibility to phishing and social engineering attacks, particularly within Nigeria's rapidly expanding digital financial services environment. Cybersecurity awareness enables users to recognize fraudulent messages and deceptive online behaviour; digital competence equips users with the knowledge and skills to identify secure digital environments and avoid risky online actions; while security behaviour reflects the extent to which users adopt protective practices such as using strong passwords, enabling two-factor authentication, and verifying suspicious requests. These behavioural factors are widely recognised as critical determinants of users' ability to resist phishing and social engineering attacks, yet evidence on their combined influence in the Nigerian context remains limited.

It is against this background that this study investigates the influence of cybersecurity awareness, digital competence, and security behavior on users' exposure and susceptibility to phishing and social engineering attacks in Nigeria's digital financial services sector. By addressing this empirical gap, the study seeks to provide evidence that will support more effective user-centered cybersecurity strategies, strengthen public confidence in digital financial services, and complement existing technological approaches to combating cyber-enabled financial fraud.

Research Objectives

The main objective of this study is to examine the relationship between cybersecurity awareness, digital competence, security behaviour, and users' vulnerability to phishing and social engineering attacks in digital financial services in Nigeria. The specific objectives are to:

1. examine the relationship between cybersecurity awareness and users' vulnerability to phishing and social engineering attacks;
2. examine the relationship between digital competence and users' vulnerability to phishing and social engineering attacks;
3. examine the relationship between security behaviour and users' vulnerability to phishing and social engineering attacks; and
4. examine the combined relationship between cybersecurity awareness, digital competence, security behaviour, and users' vulnerability to phishing and social engineering attacks.

Research Hypotheses

The following null hypotheses will guide the study:

H_{01}: There is no significant relationship between users' cybersecurity awareness of phishing and social engineering attacks and their vulnerability to such attacks among users of digital financial services in Nigeria.

H_{02}: There is no significant relationship between users' digital competence and their vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria.

H_{03}: There is no significant relationship between users' security behaviour and their vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria.

H_{04}: Cybersecurity awareness, digital competence, and security behaviour have no significant combined relationship with users' vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria.

Scope of the Study

This study focuses on users of digital financial services in Nigeria, with particular emphasis on undergraduate and postgraduate students, academic and non-academic staff of universities, employees of technology-driven organizations, and bank staff who regularly use digital financial platforms. The study specifically investigates how users' awareness of phishing and social engineering attacks, digital literacy, and security

practices influence their vulnerability to phishing and social engineering attacks.

Data were collected through university mailing lists, staff and student associations, and other online platforms. These channels provided access to respondents who are active users of digital financial services and possess varying levels of digital technology exposure, thereby ensuring the collection of relevant data for examining the relationships among the study variables.

Significance of the Study

This study is significant both theoretically and practically. Theoretically, it contributes to the growing body of knowledge on cybersecurity behaviour by providing empirical evidence on the relationships among users' awareness of phishing and social engineering attacks, digital literacy, security practices, and vulnerability to phishing and social engineering attacks within the Nigerian digital financial services environment. The findings also provide additional support for behavioural and cybersecurity theories that explain users' responses to online threats.

Practically, the findings will provide valuable insights for policymakers, financial institutions, cybersecurity professionals, educational institutions, and regulatory agencies in developing evidence-based strategies to reduce users' vulnerability to phishing and social engineering attacks.

Literature Review

Phishing

Phishing is a common form of online fraud in which criminals pretend to be trusted individuals or organizations in order to obtain sensitive information from unsuspecting users. Such information may include usernames, passwords, bank account details, card information, and Bank Verification Numbers (BVN) (Jagatic et al., 2007; Gupta et al., 2018). Phishing attacks are usually carried out through emails, text messages, social media platforms, or fake websites that closely resemble those of legitimate financial institutions.

The main goal of phishing is to deceive users into believing that a message or request is genuine. Fraudsters often copy the logos, language, and appearance of banks and other financial service providers to make their messages look authentic. Rather than attacking computer systems directly, phishing relies on tricking people into voluntarily providing confidential information. In Nigeria, the increasing use of mobile banking and digital payment systems has created more opportunities for such attacks (Akinwale & Kyari, 2020).

Closely related to phishing is social engineering. Social engineering involves manipulating individuals into revealing confidential information or taking actions that may compromise their security (Mitnick & Simon, 2002; Hadnagy, 2011). Unlike technical attacks that focus on software or network weaknesses, social engineering targets human behaviour. Fraudsters take advantage of emotions such as trust, fear, curiosity, or urgency to influence their victims.

Social engineering can take different forms, including impersonation, fake investment offers, deceptive phone calls, and requests for account verification. In many cases, attackers present themselves as bank officials, customer service representatives, or other trusted persons in order to gain access to sensitive information. (Omodunbi et al., 2016).

The growth of digital financial systems has also contributed to the increasing relevance of phishing and social engineering attacks. A digital financial system refers to the use of technology to provide financial services electronically. It includes services such as mobile banking, internet banking, electronic funds transfers, point-of-sale (POS) transactions, mobile money services, and digital wallets (Ozili, 2018; World Bank, 2020). These services have made financial transactions faster, easier, and more accessible to millions of people.

In Nigeria, digital financial services have expanded rapidly due to technological innovation, regulatory support, and the widespread use of mobile phones (Central Bank of Nigeria, 2021). While these developments have improved financial inclusion, they have also created new security challenges.

The operation of digital financial systems depends largely on Information and Communication Technology (ICT). ICT refers to the technologies used for creating, storing, processing, and sharing information. These technologies include computers, mobile devices, software applications, communication networks, and internet services (Laudon & Laudon, 2018). ICT makes it possible for individuals and organizations to communicate and conduct transactions efficiently across different locations.

Although ICT has brought significant benefits, it has also created opportunities for cybercriminals to develop more sophisticated methods of attack. (Krombholz et al., 2015). This highlights the need for stronger cybersecurity measures and continuous user education.

Theoretical Framework

This study is anchored on an integrated theoretical framework that combines ideas from psychology, criminology, information systems, and cybersecurity. The use of multiple theories is necessary because phishing and social engineering attacks are complex issues that involve human behavior, technology, and criminal activities. No single

theory can adequately explain all the factors that make individuals vulnerable to these attacks.

At the psychological level, the study draws from the Heuristic–Systematic Model (HSM) developed by Chaiken (1980) and the Elaboration Likelihood Model (ELM) proposed by Petty and Cacioppo (1986). According to the theories, individuals sometimes make quick judgments based on simple cues rather than carefully analyzing information. In the context of phishing attacks, users may trust messages simply because they appear to come from a bank or another trusted institution.

The study also adopts Cognitive Bias Theory developed by Kahneman and Tversky (1974). The theory explains that people often rely on mental shortcuts when making decisions. Individuals may be influenced by authority, familiarity, or urgency without properly evaluating the risks involved. This makes them more vulnerable to phishing and social engineering attacks.

Another relevant theory is the Protection Motivation Theory (PMT) introduced by Rogers (1975). The theory suggests that people are more likely to take protective actions when they believe a threat is serious and when they have confidence in their ability to prevent it.

From a criminological perspective, the study is supported by the Routine Activity Theory developed by Cohen and Felson (1979). The theory argues that crime occurs when a motivated offender encounters a suitable target in the absence of adequate protection.

The Fraud Triangle Theory proposed by Cressey (1953) also helps explain cybercrime. According to the theory, fraudulent behavior is influenced by pressure, opportunity, and rationalization. The availability of digital technologies, combined with economic pressures and opportunities for financial gain, contributes to the growth of phishing and social engineering attacks.

The study further draws from the Technology Acceptance Model (TAM) developed by Davis (1989). The model explains that people adopt technology when they perceive it to be useful and easy to use.

In addition, the Socio-Technical Systems Theory emphasizes the interaction between people, technology, and organizational processes. The theory suggests that weaknesses in any of these areas can create security challenges. Poor user awareness, weak security systems, or inadequate institutional controls may therefore increase vulnerability to cyberattacks.

The study is also guided by Deception Theory, which explains how fraudsters deliberately create false impressions in order to mislead their victims. Phishing attacks often succeed because attackers imitate legitimate organizations and create messages

that appear genuine. Closely related to this is the Social Engineering Framework, which explains how criminals manipulate human emotions such as trust, fear, curiosity, and urgency to obtain confidential information.

Taken together, these theories provide a comprehensive explanation of phishing and social engineering attacks. They show that cyber fraud is not only a technological problem but also a human and organizational challenge.

Empirical Review

The table below is an empirical review covering the period 2020–2025, with emphasis on Nigeria.

Table 1: Prior related studies

Author(s) & Year	Country	Focus of Study	Methodology	Major Findings	Gap Identified
Akinwale and Kyari (2022)	Nigeria	Examined cyber fraud and phishing techniques in Nigerian banking institutions.	Survey design involving bank customers and ICT personnel .	Phishing attacks have become increasingly sophisticated due to poor public awareness and inadequate cybersecurity education.	Focused mainly on banking institutions and technical countermeasures. Human behavioral factors such as digital literacy and security behavior were not comprehensively examined.
Omodunbi et al. (2020)	Nigeria	Investigated cybersecurity threats affecting electronic banking systems.	Descriptive survey with secondary cybercrime reports.	Phishing and identity theft constitutes major threats to electronic payment systems.	Concentrated on institutional vulnerabilities rather than individual users' behavioral characteristics influencing phishing susceptibility.
Adebayo and Ibrahim	Nigeria	Investigated determinants of	Questionnaire survey	Customer awareness	Digital literacy was not

Author(s) & Year	**Country**	**Focus of Study**	**Methodology**	**Major Findings**	**Gap Identified**
(2022)		cyber fraud among digital banking customers.	analysed using Structural Equation Modelling (SEM).	significantly reduced exposure to online banking fraud, while poor security practices increased fraud occurrence.	incorporated as an explanatory variable, and phishing was treated broadly as cyber fraud without isolating social engineering attacks
Adepoju et al. (2023)	Nigeria	Examined cybersecurity awareness among university students using digital financial platforms.	Cross-sectional survey .	Students with better cybersecurity education were less likely to disclose sensitive financial information online.	Limited to university students and excluded bank customers, employees and other categories of digital financial service users
Central Bank of Nigeria (2023)	Nigeria	Reported trends in electronic payment fraud within Nigeria's financial sector .	National fraud statistics and regulatory reports.	Increase in Electronic payment fraud despite improvements in banking security infrastructure. Social engineering accounted for a significant proportion of fraud incidents.	Regulatory statistics explain fraud trends but do not investigate behavioural factors responsible for users' vulnerability

Author(s) & Year	Country	Focus of Study	Methodology	Major Findings	Gap Identified
Eze and Okeke (2024)	Nigeria	Assessed the influence of cybersecurity awareness campaigns on digital banking security .	Survey and regression analysis .	Awareness programs significantly improved customers' ability to recognize fraudulent messages and suspicious links.	Did not examine digital competence and failed to measure actual security behavior among users.
Akinyemi and Salami (2024)	Nigeria	Examined behavioral determinants of mobile banking security practices.	Quantitative survey analyzed using SEM.	Security behavior was a stronger predictor of online safety than demographic characteristics.	Focused on mobile banking users only and excluded broader digital financial services such as fintech platforms and mobile money services.

Source: Authors compilation

Comparative Analysis of Previous Studies

A major point of convergence among the reviewed studies is the recognition that cybersecurity is no longer solely a technological challenge but also a behavioral issue. Most authors found that user awareness significantly influences exposure to cyber threats, while stronger cybersecurity education improves users' ability to identify fraudulent communications

Despite these similarities, notable differences exist. Some studies focused primarily on institutional cybersecurity (Omodunbi et al., 2020), while others examined mobile banking security (Akinyemi & Salami, 2024). Only a few studies specifically investigated phishing attacks, and even fewer incorporated social engineering as a distinct behavioral phenomenon. Most Nigerian studies concentrated on bank customers or university students, thereby limiting the generalizability of their findings across the broader population of digital financial service users.

Identified Research Gap

The empirical literature reveals several important gaps.

Conceptual Gap: Most previous studies examined cyber fraud, electronic banking security, or fintech adoption broadly without distinguishing phishing from social engineering attacks, despite their unique behavioral characteristics.

Variable Gap: Existing studies often investigated cybersecurity awareness in isolation. Very few studies simultaneously examined awareness, digital literacy (digital competence), and security behavior as predictors of users' vulnerability to phishing and social engineering attacks.

Population Gap: Nigerian studies largely focused on bank customers, university students, or employees of financial institutions. Limited empirical evidence exists on a broader population comprising university staff, students, technology workers, bank employees, and customers who regularly use diverse digital financial services.

Methodological Gap: Several studies relied on descriptive analyses or institutional fraud reports, with relatively few employing multivariate statistical techniques to examine the joint effects of behavioral variables on cyber vulnerability.

The present study addresses these gaps by empirically examining how awareness, digital literacy, and security behavior jointly influence vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria, using a diverse sample of digital financial service users and robust inferential statistical techniques.

Methodology

The study adopted the descriptive survey research design. This was considered appropriate because it enabled the researcher to obtain relevant information directly from respondents and assess their views, experiences and behavioral patterns regarding digital safety and cyber-related exposure. The study was conducted in Nigeria within a digital environment where individuals increasingly depend on online platforms for communication, education, commerce and institutional transactions.

The population comprised individuals actively involved in digital activities and internet-based transactions within the study area. These included respondents with access to digital devices and regular interaction with digital services. A total of 225 respondents participated in the study. The respondents were selected using the purposive sampling technique. The data were obtained directly from respondents through a structured questionnaire.

Primary data were considered suitable because they provided firsthand responses

relevant to the study objectives. The questionnaire was divided into sections covering: Awareness, Digital competence, Security behavior and Vulnerability. The items were structured using a Likert-scale format ranging from:

- Strongly Agree
- Agree
- Undecided
- Disagree
- Strongly Disagree

This format enabled respondents to indicate the extent of agreement with each statement. The instrument was subjected to face and content validity.

Experts in cybersecurity and research methodology reviewed the instrument to ensure:

- clarity,
- relevance,
- appropriateness of the items,
- alignment with study objectives.

Their observations were incorporated before final administration.

Reliability was tested using Cronbach's Alpha. This was used to determine the internal consistency of the questionnaire items. The study obtained acceptable reliability levels for all constructs. Cronbach's Alpha was calculated using the formula:

$$\alpha = \frac{k}{k-1}\left(1-\frac{\sum\sigma_i^2}{\sigma_t^2}\right)$$

Where:

- **α** = Cronbach's Alpha coefficient
- **k** = Number of items in the scale
- **$\Sigma\sigma^2_i$** = Sum of the variances of individual items
- **σ^2□** = Variance of the total score formed by summing all items

The study examined the influence of users' awareness of phishing and social engineering attacks, digital competence, and security behaviour on their vulnerability to phishing and social engineering attacks. The functional relationship is expressed as:

$$V = f(A + D + S)$$

Expanded econometric form:

$$V = \beta_0 + \beta_1 A + \beta_2 D + \beta_3 S + \mu$$

Where:

- **V** = Vulnerability to phishing and social engineering attacks
- **A** = Awareness of phishing and social engineering attacks
- **D** = Digital competence
- **S** = Security behaviour
- β_0 = Constant (Intercept)
- β_1–β_3 = Regression coefficients
- μ = Error term

Data were analysed using e-views statistical tools to summarise respondents' demographic characteristics and responses to the questionnaire items. Cronbach's Alpha was employed to assess the internal consistency and reliability of the measurement scales.

Pearson Product Moment Correlation was used to determine the direction and strength of the relationships among the study variables, while Multiple Linear Regression Analysis was employed to examine the individual and combined effects of awareness of phishing and social engineering attacks, digital competence, and security behaviour on users' vulnerability to phishing and social engineering attacks.

Before estimating the regression model, the underlying assumptions of multiple regression were assessed to ensure the validity of the results. Specifically:

- **Linearity** was examined using scatterplots to confirm a linear relationship between the dependent and independent variables.
- **Multicollinearity** was assessed using the Variance Inflation Factor (VIF) and Tolerance statistics. VIF values below 10 and Tolerance values above 0.10 were considered acceptable.
- **Normality of residuals** was evaluated using Normal Probability (P–P) plots and histogram of standardized residuals.
- **Homoscedasticity** was assessed through scatterplots of standardized residuals against standardized predicted values to verify constant error variance.

Only after these assumptions were found to be satisfactorily met was the multiple regression analysis conducted. All hypotheses were tested at the 5 percent level of significance ($\alpha = 0.05$).

Data Analyses and Discussion

The results are presented in line with the study objectives.

Table 2 Reliability Test

Construct	Alpha
Awareness	0.462
Digital Competence	0.465
Security Behavior	0.848
Vulnerability	0.596

Source: E-views statistical package version 9

Table 2 presented the results of the reliability analysis using Cronbach's Alpha to assess the internal consistency of the study constructs. Security Behaviour recorded the highest reliability coefficient (α = 0.848), indicating good internal consistency and suggesting that the items measuring this construct consistently captured respondents' security-related practices. In contrast, Vulnerability produced a coefficient of 0.596, indicating relatively low internal consistency but still suggesting a moderate level of reliability for exploratory research.

The reliability coefficients for Awareness (α = 0.462) and Digital Competence (α = 0.465) were comparatively low, indicating weak internal consistency among the items used to measure these constructs. This suggests that respondents may have interpreted some questionnaire items differently or that the constructs were multidimensional in nature. Although these values fall below the conventional threshold of 0.70, the constructs were retained because the instrument had already undergone face and content validation by experts and because the study is exploratory in nature. Nevertheless, the findings suggest that future studies should refine the measurement items to improve reliability.

Test of Hypotheses

The hypotheses were tested at the 5% level of significance. H_{01}, H_{02}, and H_{03} were tested using the Pearson Product Moment Correlation results, while H_{04} was tested using the overall F-statistic from the multiple regression analysis.

Table 3: Correlation Analysis

Variables	R	Sig
Awareness – Vulnerability	.131	.049
Digital Competence – Vulnerability	.123	.066
Security Behaviour – Vulnerability	.178	.007

Source: E-views statistical package version 9

Hypothesis One

H_{01}: There is no significant relationship between users' cybersecurity awareness of phishing and social engineering attacks and their vulnerability to such attacks among users of digital financial services in Nigeria.

The correlation analysis produced a positive correlation coefficient of r = 0.131 with a significance value of p = 0.049. Since p = 0.049 is less than the 0.05 level of significance, H_{01} is rejected. The study therefore establishes that there is a statistically significant but weak positive relationship between cybersecurity awareness and users' vulnerability to phishing and social engineering attacks.

Hypothesis Two

H_{02}: There is no significant relationship between users' digital competence and their vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria.

The correlation analysis produced a positive correlation coefficient of r = 0.123 with a significance value of p = 0.066. Since p = 0.066 is greater than the 0.05 level of significance, H_{02} is not rejected. The study therefore finds that there is no statistically significant relationship between digital competence and users' vulnerability to phishing and social engineering attacks at the 5% level of significance.

Hypothesis Three

H_{03}: There is no significant relationship between users' security behaviour and their vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria.

The correlation analysis produced a positive correlation coefficient of r = 0.178 with a significance value of p = 0.007. Since p = 0.007 is less than the 0.05 level of significance, H_{03} is rejected. The study therefore establishes that there is a statistically significant but weak positive relationship between security behaviour and users' vulnerability to phishing and social engineering attacks.

Hypothesis Four

H_{04}: Cybersecurity awareness, digital competence, and security behaviour have no significant combined relationship with users' vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria.

Table 4: Regression Analysis

Variable	Beta	Sig
Constant	5.688	.000
Awareness	.091	.383
Digital Competence	.074	.422
Security Behavior	.179	.054

Source: E-views statistical package version 9

The multiple regression model in table 4, produced an F-statistic of 3.084 with a significance value of p = 0.028. Since p = 0.028 is less than the 0.05 level of significance, H_{04} is rejected. The result indicates that cybersecurity awareness, digital competence, and security behaviour, when considered jointly, are statistically associated with users' vulnerability to phishing and social engineering attacks. However, the model explains only 4.0% of the variation in vulnerability ($R^2 = 0.040$), indicating limited explanatory power. Furthermore, none of the individual predictors was statistically significant at the 5% level.

Summary, Conclusion, Recommendations and Policy Implication.

This study examined the relationship between cybersecurity awareness, digital competence, security behaviour, and users' vulnerability to phishing and social engineering attacks among users of digital financial services in Nigeria. The major findings of the study are summarised as follows:

1. The reliability analysis revealed varying levels of internal consistency among the study constructs. Security Behaviour recorded a satisfactory reliability coefficient (Cronbach's Alpha = 0.848), indicating good internal consistency. However, Awareness ($\alpha = 0.462$), Digital Competence ($\alpha = 0.465$), and Vulnerability ($\alpha = 0.596$) recorded relatively low reliability coefficients, indicating the need for further refinement and validation of the measurement items.
2. The correlation analysis revealed a weak positive and statistically significant relationship between cybersecurity awareness and users' vulnerability to phishing and social engineering attacks ($r = 0.131$, $p = 0.049$). Thus, the study established a statistically significant but weak bivariate relationship between cybersecurity awareness and vulnerability.
3. Digital competence exhibited a weak positive relationship with users' vulnerability

($r = 0.123$), but the relationship was not statistically significant at the 5% level ($p = 0.066$). Therefore, the study did not establish a statistically significant bivariate relationship between digital competence and users' vulnerability to phishing and social engineering attacks.

4. Security behaviour recorded the strongest bivariate relationship with users' vulnerability among the three explanatory variables ($r = 0.178$, $p = 0.007$). Although the relationship was statistically significant, its magnitude remained weak. Thus, the study established a statistically significant but weak bivariate relationship between security behaviour and vulnerability.
5. The multiple regression analysis produced a statistically significant overall model ($F = 3.084$, $p = 0.028$). This indicates that cybersecurity awareness, digital competence, and security behaviour, when considered jointly, were statistically associated with users' vulnerability to phishing and social engineering attacks. However, the model explained only 4.0% of the variation in vulnerability ($R^2 = 0.040$), indicating that the explanatory power of the model was limited and that approximately 96% of the variation remained unexplained.
6. Examination of the individual regression coefficients showed that none of the three explanatory variables made a statistically significant independent contribution to vulnerability at the 5% level. Cybersecurity awareness recorded $\beta = 0.091$ ($p = 0.383$), digital competence recorded $\beta = 0.074$ ($p = 0.422$), while security behaviour recorded $\beta = 0.179$ ($p = 0.054$). Although security behaviour had the largest regression coefficient, its p-value remained above the 0.05 threshold and was therefore not statistically significant at the conventional 5% level.
7. The findings demonstrate an important distinction between the correlation and regression results. Cybersecurity awareness and security behaviour showed statistically significant bivariate relationships with vulnerability, whereas neither demonstrated a statistically significant independent effect in the multiple regression model.

Conclusion and Recommendations

This study examined the relationship between cybersecurity awareness, digital competence, security behaviour, and users' vulnerability to phishing and social engineering attacks in Nigeria's digital financial services sector. The findings provide limited evidence concerning the explanatory role of the three variables examined.

The correlation analysis revealed weak positive associations between vulnerability and both cybersecurity awareness and security behaviour, with the relationships being statistically significant. Digital competence also showed a weak positive association with vulnerability, but the relationship was not statistically significant. These bivariate

results indicate that some relationships exist among the variables, but the relatively small correlation coefficients demonstrate that the associations are weak.

The multiple regression results provide a more cautious interpretation. Although the overall regression model was statistically significant ($F = 3.084$, $p = 0.028$), the model explained only 4.0% of the variation in vulnerability ($R^2 = 0.040$). More importantly, none of the individual predictors was statistically significant at the 5% level. Awareness ($\beta = 0.091$, $p = 0.383$), digital competence ($\beta = 0.074$, $p = 0.422$), and security behaviour ($\beta = 0.179$, $p = 0.054$) therefore did not demonstrate statistically significant independent predictive effects on vulnerability.

The study consequently does not provide sufficient empirical evidence to conclude that cybersecurity awareness, digital competence, or security behaviour independently predicts users' vulnerability to phishing and social engineering attacks at the conventional 5% significance level. The difference between the correlation and regression findings further demonstrates the importance of distinguishing between simple bivariate associations and independent multivariate effects.

The low explanatory power of the regression model suggests that vulnerability to phishing and social engineering attacks is a multifaceted phenomenon that extends beyond the three variables examined. Behavioural, psychological, technological, institutional, environmental, and situational factors may also contribute to users' vulnerability. These factors were not directly examined in the present study and therefore require further empirical investigation.

Based on the findings of this study, the following recommendations are made:

1. Financial institutions should strengthen continuous, threat-specific cybersecurity awareness programmes.
2. Educational institutions and financial service providers should emphasise practical digital competence and cybersecurity education.
3. Financial institutions and organisations should promote secure digital practices among users and employees. Accordingly, secure practices such as careful verification of suspicious communications, strong authentication practices, and prompt reporting of suspected phishing attempts should be promoted as precautionary measures.
4. Financial service providers should strengthen technological and institutional safeguards.
5. Future researchers should refine the measurement instruments used to assess cybersecurity awareness, digital competence, and vulnerability. The relatively low Cronbach's Alpha coefficients indicate the need for improved measurement instruments and further validation.
6. Future studies should incorporate additional determinants of vulnerability. Since

the present regression model explained only 4.0% of the variation in vulnerability.

Policy Recommendations

Given the weak relationships and the low explanatory power of the regression model, policy interventions should adopt an integrated rather than single-factor approach.

1. The Central Bank of Nigeria, in collaboration with financial institutions, should promote minimum cybersecurity awareness standards for users of digital financial services.
2. NITDA and other relevant stakeholders should support standardised digital competence and cybersecurity education programmes
3. Financial institutions should incorporate practical cybersecurity guidance into customer onboarding and continuing customer engagement.
4. Regulatory authorities should require financial institutions to strengthen technological consumer-protection mechanisms.
5. Universities and tertiary institutions should mainstream practical cybersecurity education across relevant academic programmes. Such programmes should move beyond theoretical awareness and provide practical guidance on identifying suspicious digital communications, protecting personal information, and using digital financial services securely.
6. Policymakers should adopt a multi-layered cybersecurity policy framework.

References

Akinwale, Y. O., & Kyari, A. K. (2022). Factors influencing attitudes and intention to adopt financial technology services among the end-users in Lagos State, Nigeria. *African Journal of Science, Technology, Innovation and Development, 14*(1), 272–279. https://doi.org/10.1080/20421338.2020.1835177

Central Bank of Nigeria. (2021). *Annual report*. Central Bank of Nigeria.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology, 39*(5), 752–766.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions.

Telecommunication Systems, 67(2), 247–267.

Hadnagy, C. (2011). *Social engineering: The art of human hacking*. Wiley.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

Kahneman, D., & Tversky, A. (1974). Judgment under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124–1131.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122.

Laudon, K. C., & Laudon, J. P. (2018). *Management information systems: Managing the digital firm* (15th ed.). Pearson.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Wiley.

National Bureau of Statistics. (2023). *Nigerian gross domestic product report and digital economy statistics*. National Bureau of Statistics.

Nigeria Inter-Bank Settlement System. (2025). *Fraud report 2024.* Lagos, Nigeria

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *International Journal of Advanced Computer Science and Applications, 7*(5), 371–379.

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review, 18*(4), 329–340.

Petty, R. E., & Cacioppo, J. T. (1986). *Communication and persuasion: Central and peripheral routes to attitude change*. Springer-Verlag.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.

Verizon. (2024). *2024 Data breach investigations report*. Verizon.

World Bank. (2020). *Digital financial services*. World Bank.