

**ANUK COLLEGE OF  
PRIVATE SECTOR  
Accounting Journal**

**VOL. 2 NO. 4 DECEMBER, 2025**

**A Publication of College of Private Sector  
Accounting  
ANAN University Kwall, Plateau State, Nigeria.**

Copyright © College of Private Sector ANAN University Kwall, Plateau State, Nigeria.

Published December, 2025.

Web Address: <https://www.anukpsaj.com>, Email: [anukpsaj@gmail.com](mailto:anukpsaj@gmail.com)

All right reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission of the copyright owner,

Printed by:  
**MUSSAB Printers,**  
NB, 9 Muri road by gwari road, Kaduna State, Nigeria.  
**Phone contact:** 07038776658,  
**Email:** [meetsuleiman009@gmail.com](mailto:meetsuleiman009@gmail.com)

## **Structure of Manuscript**

Manuscripts must be typed on A size paper with 12 font size (Times New Roman), not more than 15 pages, double-spaced, and in English. The file name should include the corresponding author's name and a keyword from the title.

### **Sequence of Manuscript**

- I. Title page
- II. Abstract (150-250 words)
- III. Keywords (3-5)
- IV. Introduction
- V. Literature Review
- VI. Methodology
- VII. Results and Discussion
- VIII. Conclusion and Recommendations
- IX. References (APA 7th Edition)
- X. Appendices (if necessary)
- XI. Author Biographies (optional)

## **Plagiarism Policy**

ANUK is committed to maintaining high standards through an indept peer-review process with sound ethical policies. Any infringements of professional ethical codes, such as plagiarism; including self-plagiarism, fraudulent use of data, are seriously frowned at by the journal with zero tolerance.

ANUK implements the Code of Conduct of the Committee on Publication Ethics (COPE), and uses the COPE Flowcharts for Resolving cases of suspected plagiarism or any publication misconduct.

In order to avoid plagiarism cases with the ANUK, the following guidelines must be strictly adhered to by authors:

Authors should ensure that they have written entirely original works, and if authors have used the work and/or words of others that this has been appropriately cited or quoted.

An author should not, in general, publish manuscripts describing essentially the same research in more than one journal or primary publication. Submitting the same manuscript to more than one journal concurrently constitutes unethical publishing behavior and is unacceptable.

Proper acknowledgment of the work of others must always be adhered to. Authors should cite publications that have been influential in determining the nature of the reported work.

## Editorial Team

### Editor-in-Chief :

**Prof. Musa Adeiza Farouk**

Dean, College of Private Sector Accounting  
ANAN University Kwall, Plateau State.

### Associate Editor:

**Dr. Saidu Halidu**

Department of Financial Reporting,  
ANAN University Kwall, Plateau State.

### Managing Editor :

**Dr. Abubakar Ahmed**

College of Private Sector Accounting,  
ANAN University Kwall, Plateau State.

## Members Editorial Board

**Prof. Joseph Femi Adebisi**

DVC ANAN University Kwall, Plateau State.

**Prof. Tamunonimim Ngereboa**

Dean, Public Sector Accounting,  
ANAN University Kwall, Plateau State.

**Prof Kabir Tahir Hamid,**

Department of Accounting,  
Bayero University, Kano, Kano State.

**Prof. Ekoja B. Ekoja,**

Department of Accounting,  
University of Jos.

**Prof. Clifford Ofurum,**

Department of Accounting,  
University of Port Harcourt, Rivers State.

**Prof. Ahmad Bello Dogarawa,**

Department of Accounting,  
Ahmadu Bello University Zaria.

**Prof. Muhammad Junaidu Kurawa,**

Department of Accounting,  
Bayero University Kano, Kano State.

**Prof. Muhammad Habibu Sabari,**

Department of Accounting,  
Ahmadu Bello University, Zaria.

**Prof. Hassan Ibrahim,**

Department of Accounting,  
IBB University, Lapai, Niger State.

**Prof. Tochukwu Okafor,**

Department of Accounting,  
University of Nigeria, Nsukka.

**Prof. Muhammad Aminu Isa,**

Department of Accounting,  
Bayero University, Kano, Kano State.

**Prof. Ahmadu Bello,**

Department of Accounting,  
Ahmadu Bello University, Zaria.

**Prof. Musa Yelwa Abubakar,**

Department of Accounting,  
Usmanu Danfodiyo University, Sokoto State.

**Prof. Salisu Abubakar,**

Department of Accounting,  
Ahmadu Bello University Zaria, Kaduna State.

**Prof. Isaq Alhaji Samaila,**

Department of Accounting,  
Bayero University, Kano State.

**Prof. J.J. Adefila,**

Department of Accounting,  
University of Maidugu, Borno State.

**Prof. Chinedu Innocent Enekwe,**

Department of Financial Management,  
ANAN University Kwall, Plateau State.

**Dr. Dang Yohanna Dagwom,**

Department of Public Sector Accounting,  
ANAN University Kwall, Plateau State.

**Dr. Abdulrahman Abubakar,**  
Department of Accounting,  
Ahmadu Bello University Zaria.

**Dr. Aisha Nuhu Muhammad,**  
Department of Accounting,  
Ahmadu Bello University Zaria.

**Dr. Abubakar Ahmad,**  
School of Business and Entrepreneurship,  
Amerian University of Nigeria, Yola.

**Dr. Suleiman Salami,**  
Department of Accounting,  
ABU Business School,  
Ahmadu Bello University Zaria.

**Prof. Sunday Mlanga,**  
Director Academic Planning,  
ANAN University Kwall Plateau State

**Dr. Saheed Adebowale Nurein,**  
School of Business and Entrepreneurship,  
Amerian University of Nigeria, Yola.

**Prof. Isaq Alhaji Samaila,**  
Department of Accounting,  
Bayero University, Kano.

**Dr. Maryam Isyaku Muhammad**  
Department of Accountancy,  
Federal University of Technology, Yola

**Dr. Latifat Muhibudeen,**  
Department of Accounting,  
Yusuf Maitama Sule University, Kano

#### Advisory Board Members

**Prof. Musa Inuwa Fodio,**  
V.C, ANAN University Kwall,  
Plateau State

**Prof. Kabiru Isah Dandago,**  
Bayero University Kano,  
Kano State.

**Prof. Suleiman A. S. Aruwa,**  
Department of Accounting,  
Nasarawa State University, Keffi,  
Nasarawa State.

**Prof. A.M Bashir,**  
Usmanu Danfodiyo University Sokoto,  
Sokoto State.

**Prof. Muhammad Tanko,**  
Kaduna State University, Kaduna.

**Prof. Bayero A.M Sabir,**  
Usmanu Danfodiyo University Sokoto,  
Sokoto State.

**Prof. Aliyu Sulaiman Kantudu,**  
Bayero University Kano, Kano State.

**Prof. B.C Osisioma,**  
Department of Accounting,  
Nnamdi Azikwe University, Akwa

**Prof. M.A. Mainoma,**  
Department of Accounting,  
Nasarawa State University, Keffi

**Prof. J. C Okoye,**  
Department of Accounting,  
Nnamdi Azikwe University, Akwa

**Prof. J.O. N Ande,**  
Department of Accounting, University of Jos.

**Prof. Shehu Usman Hassan,**  
Dean Faculty of Management Science,  
Federal University of Kashere, Gombe State.

#### Editorial Secretary

**Dr. Benjamin David Uyagu**  
Department of Auditing and Forensic Accounting,  
ANAN University Kwall, Plateau State.

## TABLE OF CONTENT

1. <b>Effect of Firm Characteristics on Firm Value of Listed Deposit Money Banks in Sub-saharan Africa</b> .....	1
Mabur Zungbung Danladi, Deshi Nentawe Nengak, Maren Maram Isah and Dahel Innocent Felix	
2. <b>Effect of Forensic Interviews And Fund Tracing Techniques on Fraud Control in Public Sector Pension Administration in Kebbi State, Nigeria</b> .....	17
Ahmed Yarima Dakingari, Attahiru Ibrahim Alkali and Zainab Attahiru Alkali	
3. <b>Audit Quality as a Moderator Between Board Characteristics and Earnings Management: Evidence From Listed Banks in Nigeria</b> .....	25
Sabiu Ishaka Alfa, Lawal Faith Chidinma and Musa Adeiza Farouk	
4. <b>Effect of Non-current Assets on Value of Listed Consumer Goods Firms in Nigeria</b> .....	37
Mabur Zungbung Danladi, Deshi Nentawe Nengak, Maren Maram Isah and Dahel Innocent Felix	
5. <b>Effect of Forensic Accounting Techniques on Fraud Prevention In Ministries, Departments And Agencies (MDAs) in Plateau State</b> .....	51
Ondeku Felix Godwin, Adebisi Joseph Femi and Farouk Musa Adeiza	
6. <b>Effect of Forensic Interviews And Fund Tracing Techniques on Fraud Control in Public Sector Pension Administration in Kebbi State, Nigeria</b> .....	62
Ahmed Yarima Dakingari, Attahiru Ibrahim Alkali, Zainab Attahiru Alkali and Balkisu Ahmad Maiahu	
7. <b>Effect of Auditor Skills on Financial Accountability of Plateau State Government Ministries</b> .....	71
Umar Aishatu Adam	
8. <b>Effect of Ownership Structure on Environmental Disclosures of Listed Oil And Gas Companies in Nigeria</b> .....	80
Deshi Nentawe Nengak and Manji Eugene Nenkanma Helen	
9. <b>Moderating Effect of Audit Quality on Board Characteristics And Earnings Management of Listed Insurance Firms in Nigeria</b> .....	94
Sabiu Ishaka Alfa, Joseph Femi Adebisi, Musa Adeiza Farouk and Audu K. Buba	
10. <b>Effect of Board Characteristics on Cash Holding of Listed Commercial Banks in Nigeria</b> .....	105
Cycle Florence Kemebinkedoumene	
11. <b>Effect of Accounting Information Systems on Financial Reporting Quality of Listed Deposit Money Banks in Nigeria</b> .....	115
Adewole Adefemi Kazeem, Tamunonimim Ngerebo and Innocent Chinedu Enekwé	
12. <b>Effect of Corporate Governance Attributes and Value of Listed Insurance Companies in Nigeria</b> .....	126
Ahmed Tijjani Haruna	
13. <b>Effect of Forensic Accounting Tools on Fraud Prosecution Process in Nigeria Court System</b> .....	138
Blessing Chinelu Chukwu	

## TABLE OF CONTENT

14. <b>Effect of Sustainability Reporting on Share Price of Listed Oil and Gas Firms in Nigeria</b> .....	148
Clement Osemwengie Ekhoe-ugiagbe and Ojeifo Sidney Imevbore	
15. <b>Moderating Effect of Information Communication Technology Software on The Relationship Between Ownership Structure and Value of Listed Financial Firms in Nigeria</b> .....	160
Ejike Emeka Okongwu, Benjamin Uyagu and Farouk Musa Adeiza	
16. <b>Effect of Government Integrated Financial Management Information System Implementation on Financial Governance in Selected Ministries, Departments, and Agencies in Nigeria</b> .....	176
Emmanuel Monday Essien	
17. <b>Effect of Accounting Practices on Budget Implementation of Government-owned Research Institutes in South Eastern Nigeria</b> .....	194
Dennis Nnenna Okoro	
18. <b>Moderating Effect of Internal Audit Quality on The Relationship Between Accounting Information Systems and Financial Reporting Quality of Listed Deposit Money Banks in Nigeria</b> .....	205
Adewole Adefemi Kazeem, Tamunonimim Ngerebo and Innocent Chinedu Enekwe	
19. <b>Effect of Board Audit Committee Attributes on Assets Fraud Detection among Listed Manufacturing Companies in Nigeria</b> .....	215
Agboide Sunday Theophilus	
20. <b>An Empirical Analysis of The Relationship Between Government Transfer Payments and Economic Growth in Nigeria</b> .....	224
Inuwa Auwalu, Uyagu David Benjamin and Ganiyu A. Mustapha	
21. <b>Effect of Budget Processes on Performance of Public Funds in Plateau State Ministries, Departments and Agencies</b> .....	234
Yaks Mary Benjamin	
22. <b>The Effect of Cyber Fraud on Customer Trust in Nigerian Deposit Money Banks: A Digital Forensic Perspective</b> .....	250
Nkwonta Ifeoma Nnenna, Musa Adeiza Farouk and Benjamin Uyagu David	
23. <b>Effect of Forensic Audit on Fraud Detection in The Federal Ministry of Finance and Associate Agencies in Nigeria</b> .....	258
Musa Inuwa Fodio, Benjamin Uyagu David and Sani Chida Baba	
24. <b>Dividend Policy Determinants: Likelihood and Payout Magnitude in Nigeria's Consumer Goods Firms</b> .....	269
Ovbe Simon Akpadaka	
25. <b>Effect of Monetary Policy Instruments on Capital Adequacy of Listed Deposit Money Banks in Nigeria</b> .....	284
Jadesola Regina Adekalu, Joseph Femi Adebisi, Mbatuegwu David Christopher and Samuel Olutokunbo Adekalu	

## TABLE OF CONTENT

26. <b>Effect of Economic, Social and Governance Disclosures on Firm Value And The Moderating Effect of Leverage. A Study of Listed Non-financial Firms in Nigeria</b> .....	293
Aishat Oyiza Otori	
27. <b>Monetary Policy, Bank Size, and Capital Adequacy: A Conceptual Framework For Financial Stability in Nigeria</b> .....	301
Jadesola Regina Adekalu, Joseph Femi Adebisi, Mbatuegwu David Christopher and Samuel Olutokunbo Adekalu	
28. <b>Impact of Money Laundering Activities on The Operational Performance of Listed Commercial Banks in Nigeria</b> .....	312
Inuwa Auwalu and Ganiyu A. Mustapha	
29. <b>Effect of Computerized Forensic Investigation Techniques on Fraud Management in Lagos State Ministries, Departments and Agencies ...</b>	320
Kotun Rasheetdat Bunmi, Sunday Mlanga and Halidu Saidu	
30. <b>Moderating Effect of Bank Size on The Relationship Between Monetary Policy and Capital Adequacy of Listed Deposit Money Banks in Nigeria</b> ....	336
Jadesola Regina Adekalu, Joseph Femi Adebisi, Mbatuegwu David Christopher and Samuel Olutokunbo Adekalu	
31. <b>Legislative and Audit Oversight Institutions as Determinants of Budget Transparency in Sub-saharan Africa</b> .....	350
Emmanuel Sani	
32. <b>Do Sustainability Disclosures Matter For Market Valuation? Evidence From Consumer Goods Firms in Sub-saharan Africa</b> .....	358
Oloruntoba Adebayo Femi, Dagwon Yohanna Dang and Joseph Femi Adebisi	
33. <b>Effect of Monetary Policy on Manufacturing Outputs in Nigeria: 1980-2024</b> .....	368
S.A.S Aruwa, Benjamin Uyagu and Egbo Roseline Oruaroghene	
34. <b>Determinants of Public Participation in Public Budgeting among Sub-saharan Countries: The Influence Of Transparency and Oversight Institutions</b> .....	382
Emmanuel Sani	

# THE EFFECT OF CYBER FRAUD ON CUSTOMER TRUST IN NIGERIAN DEPOSIT MONEY BANKS: A DIGITAL FORENSIC PERSPECTIVE

NKWONTA IFEOMA NNENNA

MUSA ADEIZA FAROUK

BENJAMIN UYAGU DAVID

## ABSTRACT

*This study investigated the effect of cyber fraud on customer trust in Nigerian deposit money banks, focusing specifically on phishing and online banking fraud, from a digital forensic perspective. A survey research design was adopted, with 348 respondents, including bank customers and staff, providing data through structured questionnaires. The collected data were analyzed using descriptive statistics and multiple regression analysis to determine the relationship between cyber fraud and customer trust. The findings revealed that both phishing and online banking fraud have a significant negative impact on customer trust, demonstrating that cyber threats undermine confidence in digital banking systems. The study further highlighted the critical role of digital forensic practices in detecting, investigating, and mitigating fraud to restore customer confidence. Based on these results, it is recommended that banks implement stronger anti-phishing measures, enhance customer awareness programs, and establish dedicated forensic units to safeguard funds and maintain trust. This study contributes to understanding the interaction between cyber fraud, digital forensic interventions, and customer trust in Nigeria's digital banking environment.*

**Keywords:** Cyber Fraud, Phishing, Online Banking Fraud, Customer Trust, Digital Forensics, Nigerian Deposit Money Banks

## 1.0 Introduction

Banking in Nigeria has undergone a profound transformation in the last two decades, driven largely by technological innovation and the rapid digitization of financial services. The introduction of mobile banking applications, internet banking platforms, and USSD codes has made financial transactions faster, more convenient, and widely accessible, contributing significantly to the Central Bank of Nigeria's cashless policy and the broader goal of financial inclusion (Soetan, & Mogaji, 2024). However, alongside these advances has emerged an equally dynamic threat: cyber fraud. As banks move more of their services online, fraudsters have exploited vulnerabilities in digital systems and, more significantly, in human behavior, to carry out sophisticated scams that undermine not only the financial stability of customers but also the trust that sustains the banking sector (Kaur *et al.* 2021).

Customer trust is the foundation upon which the banking industry is built. Without the confidence that their funds, data, and transactions are secure, customers are reluctant to fully engage with digital

platforms (Hasan *et al.* 2023). Cyber fraud represents a direct challenge to this trust, as it introduces fear, uncertainty, and reputational risks for financial institutions. Two forms of fraud have become especially prominent in the Nigerian banking environment: phishing and online banking fraud. Phishing, which relies on deceptive techniques such as fraudulent emails, SMS, or cloned websites to trick unsuspecting users into divulging sensitive information like login credentials or one-time passwords, has become pervasive because of its relatively low execution cost and high success rate. Online banking fraud, on the other hand, involves unauthorized access to customer accounts and the execution of fraudulent transactions that often result in direct financial losses. Both types of fraud have been repeatedly reported in Nigeria, with studies and media reports showing an upward trend in the frequency and sophistication of attacks (Alsayed, & Bilgrami, 2017).

The implications of these fraudulent activities are far-reaching. Beyond the immediate financial losses suffered by victims, there is an erosion of confidence

in digital banking systems. Customers who fall victim to phishing attacks may begin to doubt their ability to interact safely with online platforms, while those affected by online banking fraud often question the competence and integrity of banks in safeguarding their funds. Even customers who have not personally experienced fraud may develop apprehension when they hear of widespread cyberattacks, thereby limiting their adoption of electronic services. This lack of trust can slow the progress of digital transformation in the financial sector, reduce profitability for banks, and hinder the broader national agenda of leveraging technology for economic growth (Ripples Nigeria, 2023; Oyibo & Ifatimehin, 2024).

Digital forensics, also known as computer forensics, is a branch of forensic science that involves the identification, collection, analysis, and preservation of digital evidence from electronic devices and computer systems for the purpose of investigating and preventing cybercrimes, data breaches, and other digital-related incidents. It encompasses a wide range of techniques and methodologies aimed at uncovering, interpreting, and presenting digital evidence in a legally admissible manner (Mondaq, 2024; Onamusi et al., 2024). This study therefore examines the effect of cyber fraud measured through phishing and online banking fraud on customer trust in Nigerian deposit money banks, adopting a digital forensic perspective to highlight both the challenges and possible remedies.

Cyber fraud has become one of the most critical threats to the stability and credibility of the Nigerian banking sector. With the expansion of digital banking services, fraudsters have exploited technological vulnerabilities and human weaknesses to perpetrate phishing, identity theft, and online account manipulation. Several studies have examined the rising incidence of cyber fraud and its impact on the banking system. For instance, Adeniran and Abiola (2022) observed that cybercrime incidents have grown proportionately with the level of digitalization in Nigerian banks, resulting in substantial financial and reputational losses. Similarly, Eze and Ekwueme (2023) found that the increasing prevalence of online fraud has led to declining customer confidence and a slower rate of technology adoption.

However, much of the existing literature has primarily focused on the technological and regulatory dimensions of cyber fraud, with limited attention to its behavioral consequences, particularly how specific types of fraud such as phishing and online banking fraud affect customer trust. Studies such as Kaur et al. (2021) and Hasan et al. (2023) have examined cybersecurity awareness and data protection practices, but they often treat cyber fraud as a general phenomenon without distinguishing the effects of its subtypes on user perception and confidence.

Moreover, while digital forensic techniques are widely recognized for their importance in detecting and investigating cybercrimes, there is insufficient empirical research on how their application can help rebuild or sustain customer trust after fraud incidents. This gap in literature creates uncertainty about how Nigerian deposit money banks can strategically use digital forensics not only to investigate cyber fraud but also to reinforce public trust in digital financial platforms. Consequently, this study seeks to fill this gap by empirically examining the effect of cyber fraud—measured through phishing and online banking fraud—on customer trust in Nigerian deposit money banks, from a digital forensic perspective.

## 1.2 Objectives and Hypotheses of the Study

The broad objective of this study is to examine the effect of cyber fraud on customer trust in Nigerian deposit money banks from a digital forensic perspective.

1. To determine the effect of phishing on customer trust in Nigerian deposit money banks.
2. To examine the effect of online banking fraud on customer trust in Nigerian deposit money banks.

**H<sub>01</sub>:** Phishing has no significant effect on customer trust in Nigerian deposit money banks.

**H<sub>02</sub>:** Online banking fraud has no significant effect on customer trust in Nigerian deposit money banks.

## 2.0 Literature Review

**Phishing:** Phishing is a form of cyber fraud where attackers impersonate legitimate entities to deceive individuals into disclosing sensitive information, such as usernames, passwords, or financial details. In Nigeria, phishing attacks have become increasingly prevalent, with fraudsters leveraging social engineering tactics to exploit unsuspecting users. A notable example is the Raccoon0365 phishing service, which enabled users to conduct large-scale phishing campaigns, compromising at least 5,000 Microsoft accounts and amassing significant financial gains through cryptocurrency (Reuters, 2025). Such incidents highlight the growing sophistication of phishing schemes and their potential to undermine the security of digital banking platforms.

**Online Banking Fraud:** Online banking fraud encompasses various illicit activities conducted through digital banking channels, including unauthorized transactions, identity theft, and account takeovers. In Nigeria, the rise of mobile and internet banking has unfortunately been accompanied by an increase in cyber fraud incidents. In 2023, the Nigerian banking sector recorded approximately ₦17.67 billion in fraud-related losses, with over 50% of these incidents occurring through digital platforms (BusinessDay, 2025). This underscores the vulnerability of online banking systems and the urgent

need for robust security measures to protect customers and maintain trust in digital financial services.

**Customer Trust:** Customer trust is a fundamental component of the banking sector, influencing customer retention, satisfaction, and the overall adoption of digital banking services. The erosion of trust can have detrimental effects on the financial system, leading to reduced customer engagement and a decline in the usage of electronic payment channels. Research indicates that electronic bank fraud significantly impacts customers' trust in Nigeria, with mobile and website fraud posing more substantial threats than traditional ATM fraud (Ajayi et al., 2021). Restoring and maintaining customer trust requires banks to implement effective fraud prevention strategies, enhance digital forensic capabilities, and foster transparent communication with customers.

## 2.2 Empirical Studies

Recent empirical research underscores the significant impact of cyber fraud on customer trust in Nigerian deposit money banks. Oloyede, Akinyele, and Adejayan (2021) conducted a comprehensive study on electronic bank fraud in Nigeria and its effect on customer trust. Using logit regression analysis, the study revealed that mobile banking and website fraud pose serious threats to customers' confidence in digital banking channels. The researchers emphasized that without effective fraud detection systems and enhanced security measures, customers' trust in electronic banking is significantly compromised. Their findings highlight the critical need for banks to adopt proactive measures to prevent cyber fraud and reassure customers about the safety of digital transactions.

Umoh, Obafe, and Eze (2024) examined the broader implications of banking fraud on public trust and economic stability in Nigeria. Their study found that insider-related fraud, weak internal controls, and the increasing sophistication of cyber threats collectively erode public confidence in the banking system. They argued for a holistic approach to fraud management, combining technological solutions, rigorous internal controls, and staff training to restore trust and safeguard the integrity of financial institutions.

Wang, Zhang, and Li (2020) focused on phishing and other cyber-dependent crimes within Nigeria's internet banking sector. Their findings indicated that phishing attacks, card theft, and online banking fraud are prevalent and contribute substantially to the erosion of customer trust. The study emphasized that effective cybersecurity practices, coupled with timely detection and response mechanisms, are essential for maintaining the credibility of digital banking platforms.

Aderinto (2025) investigated the financial

implications of cybersecurity threats on the performance of listed commercial banks in Nigeria. The study revealed that banks experiencing significant cyber fraud incidents suffered negative impacts on their earnings per share and overall financial performance. The research highlighted the dual effect of cyber fraud: it not only damages customer trust but also directly undermines the financial sustainability of banks.

Cele, Adesanya, and Bello (2024) assessed the experience of Nigerian customers with e-banking services and the associated cyber risks. Their study showed that over half of the respondents had encountered some form of cyber-related threat, which led to concerns about the security of digital banking systems. These experiences were linked to reduced customer loyalty and diminished confidence in banking institutions. The study concluded that comprehensive security frameworks, combined with customer education and awareness initiatives, are vital for mitigating cyber fraud and restoring trust in digital banking services.

## 2.3 Theoretical Framework

**Fraud Triangle Theory:** The Fraud Triangle Theory, developed by Cressey (1953), explains why individuals commit fraudulent acts based on three elements: pressure, opportunity, and rationalization. In the context of digital banking, pressure may arise from financial needs or personal gain, opportunity comes from vulnerabilities in banking systems, and rationalization allows fraudsters to justify their actions. This theory is relevant to the current study as it helps explain the occurrence of phishing and online banking fraud in Nigeria. By understanding the factors that motivate cybercriminals, banks can design more effective preventive controls, monitoring systems, and digital forensic strategies to mitigate fraud and protect customer trust (Albrecht et al., 2018).

**Technology Acceptance Model (TAM):** The Technology Acceptance Model, proposed by Davis (1989), posits that users' adoption of technology is influenced by perceived usefulness and perceived ease of use. Customer trust is a crucial factor in this model because security concerns, such as phishing and online banking fraud, can negatively affect users' perceptions and willingness to engage with digital banking services. If customers perceive online platforms as unsafe, they are less likely to use them, undermining the effectiveness of technological innovations. Applying TAM in this study provides a framework for understanding how cyber fraud impacts customer trust and the subsequent adoption of digital banking channels, highlighting the role of digital forensic interventions in restoring confidence (Venkatesh & Bala, 2008).



**Trust Theory:** Trust Theory emphasizes the importance of reliability, integrity, and competence in fostering trust between institutions and their clients (Mayer, Davis, & Schoorman, 1995). In banking, trust determines whether customers feel confident that their funds and personal information are secure. Cyber fraud, particularly phishing and online banking fraud, challenges this trust by exposing weaknesses in system security and institutional oversight. The theory underlines the significance of digital forensics in demonstrating accountability, detecting breaches, and reassuring customers that banks can manage and respond effectively to cyber threats, thereby maintaining trust (Gefen, 2000).

### 3.0 Methodology

The study adopted a survey research design, utilizing primary data collection through structured questionnaires. This approach enabled the collection of relevant information directly from customers and banking personnel in selected Nigerian deposit money banks. The survey focused on understanding the prevalence and effects of phishing and online banking fraud on customer trust, as well as the role of digital forensic practices in mitigating these effects. By using a survey design, the study could efficiently capture perceptions, experiences, and insights from respondents, providing empirical evidence on the relationship between cyber fraud and customer trust in the digital banking environment. The study relied primarily on primary data, collected directly from respondents through structured questionnaires. This

approach allowed for the direct gathering of relevant information from customers and key personnel of selected deposit money banks in Nigeria. The questionnaires were carefully designed to capture respondents' experiences and perceptions regarding phishing, online banking fraud, and customer trust, as well as the role of digital forensic practices in detecting, investigating, and mitigating cyber fraud. This method ensured that the study obtained first-hand insights on how cyber fraud affects customer confidence and the effectiveness of forensic interventions in maintaining trust in digital banking systems. The population of this study comprises customers and staff of selected Nigerian deposit money banks who interact with digital banking platforms. This includes account holders, branch managers, IT personnel, and compliance officers who have direct experience with online banking services and exposure to cyber fraud. Focusing on these groups ensures that the study captures insights from both the users of digital banking systems and those responsible for managing security and operational controls. The study selected five prominent deposit money banks in Nigeria to represent the population: Access Bank Plc, Guaranty Trust Bank Plc, Zenith Bank Plc, First Bank of Nigeria Plc, and United Bank for Africa Plc. The population distribution across these banks is presented in the table below.

**Table 1: Population Distribution Across Selected Banks**

Bank Name	Customers	Staff	Total Population
Access Bank Plc	500	50	550
Guaranty Trust Bank Plc	450	45	495
Zenith Bank Plc	480	48	528
First Bank of Nigeria Plc	520	52	572
United Bank for Africa Plc	470	47	517
<b>Total</b>	<b>2420</b>	<b>242</b>	<b>2662</b>

Source: Field Survey, 2025.

#### Sample Size Determination

The total population of the study is 2,662 (customers and staff across the selected banks). To determine a representative sample size, Taro Yamane's (1967) formula is used:

Where:  
 n = sample size  
 N = population size  
 e = margin of error (5% or 0.05)

$$n = \frac{N}{1 + N(e)^2}$$

$$n = \frac{2662}{7.655} \approx 347.8$$

The sample size is approximately 348 respondents. The study used simple random sampling to select respondents. This technique ensured that every participant had an equal chance of being chosen, minimizing bias and enhancing the validity and reliability of the results. The study employed

descriptive and inferential statistical techniques to analyze the collected data. Descriptive statistics, including frequency tables and percentages, were used to summarize respondents' demographic characteristics and their experiences with phishing and online banking fraud. Inferential analysis was



conducted using multiple regression analysis to examine the relationship between cyber fraud (measured as phishing and online banking fraud) and customer trust in Nigerian deposit money banks. Multiple regression was chosen because it allows the assessment of the combined effect of multiple independent variables (phishing and online banking fraud) on a dependent variable (customer trust), while controlling for potential confounding factors. This approach enables the study to determine not only the significance of each type of cyber fraud but also the extent to which digital forensic measures can mitigate the negative effects of these frauds on customer

confidence in digital banking platforms.

**3.2 Variables Measurements**

The study involved three key variables: phishing, online banking fraud, and customer trust. The variables were measured based on respondents' perceptions and experiences using structured questionnaire items on a Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). The measurement of each variable is described in the table below.

Variables	Measurements
Phishing	Respondents' perceptions of the prevalence and impact of phishing on their trust in the bank.
Online Banking Fraud	Respondents' experiences and views on how online banking fraud affects their confidence in using digital banking services.
Customer Trust	The level of confidence, satisfaction, and reliance customers have in the bank's ability to secure their funds and personal information.

**Model Specification:** To examine the effect of cyber fraud on customer trust, the study employed a multiple regression model, where customer trust is the dependent variable and phishing and online banking fraud are the independent variables. The model is specified as follows:

$$CT = \beta_0 + \beta_1PH + \beta_2OBF + \epsilon$$

Where:

- CT = Customer Trust (dependent variable)
- PH = Phishing (independent variable)
- OBF = Online Banking Fraud (independent variable)
- $\beta_0$  = Intercept of the model
- $\beta_1, \beta_2$  = Coefficients of the independent variables
- $\epsilon$  = Error term

**4.0 Results and Discussion**

A total of 348 questionnaires were administered to respondents, based on the previously determined sample size using Taro Yamane's formula. Out of these, 341 questionnaires were completed and returned, yielding a response rate of 97.99%. This high response rate demonstrates strong cooperation from both bank customers and staff, enhancing the reliability and representativeness of the data for analyzing the effects of phishing and online banking fraud on customer trust, as well as the mitigating role of digital forensic practices in Nigerian deposit money

banks.

**4.2 Test of Hypotheses**

In this section, the study examined the stated hypotheses using the established decision rules. The collected data were analyzed through multiple regression analysis, and the probability (p-value) statistics were applied to determine whether to accept or reject each null hypothesis. This approach allowed for an empirical assessment of the relationship between phishing, online banking fraud, and customer trust in Nigerian deposit money banks.

**Hypothesis One**

**H<sub>01</sub>:** Phishing has no significant effect on customer trust in Nigerian deposit money banks.

**Dependent Variable:** Customer Trust (CT)

**Method:** Least Squares

Variable	Coefficient ( $\hat{\alpha}$ )	Std. Error	t-Statistic	Prob.
C	2.105	0.210	10.024	0.000
PH	-0.432	0.087	-4.966	0.000

**Source:** Researcher's Computation Using E-views

The regression results show that phishing (PH) has a negative and statistically significant effect on customer trust at the 5% significance level ( $\beta = -0.432, p = 0.000$ ). Since the p-value is less than 0.05, the null hypothesis (H<sub>01</sub>: Phishing has no significant effect on customer trust) is rejected.



This indicates that as exposure to phishing increases, customer trust in Nigerian deposit money banks significantly decreases, highlighting the critical need for banks to implement effective digital forensic and cybersecurity measures to protect customers and maintain confidence in digital banking platforms.

**Hypothesis Two**

**H<sub>02</sub>:** Online banking fraud has no significant effect on customer trust in Nigerian deposit money banks.

**Dependent Variable:** Customer Trust (CT)

**Method:** Least Squares

Variable	Coefficient (â)	Std. Error	t-Statistic	Prob.
C	2.032	0.198	10.263	0.000
OBF	-0.387	0.092	-4.207	0.000

**Source:** Researcher’s Computation Using E-views

The regression results indicate that online banking fraud (OBF) has a negative and statistically significant effect on customer trust at the 5% significance level ( $\beta = -0.387, p = 0.000$ ). Since the p-value is below 0.05, the null hypothesis ( $H_{02}$ : Online Banking Fraud has no significant effect on customer trust) is rejected. This finding suggests that incidents of online banking fraud significantly reduce customers' confidence in Nigerian deposit money banks, emphasizing the importance of digital forensic interventions and robust cybersecurity measures to protect customer funds and restore trust in digital banking services.

**4.3 Discussion of Findings**

The findings of this study revealed that both phishing and online banking fraud have significant negative effects on customer trust in Nigerian deposit money banks. The regression results indicated that phishing has a strong inverse relationship with customer trust, with a coefficient of -0.432 and a p-value of 0.000, leading to the rejection of the null hypothesis ( $H_{01}$ ). This finding aligns with previous studies that have highlighted phishing as a major threat to digital banking security. For instance, Wang, Zhang, and Li (2020) noted that phishing attacks exploit vulnerabilities in customer behavior, leading to financial loss and diminished confidence in banking platforms. Similarly, Oloyede, Akinyele, and Adejayan (2021) observed that phishing undermines the perceived integrity of banks, causing customers to hesitate in adopting online banking services.

The study also found that online banking fraud significantly reduces customer trust ( $\beta = -0.387, p = 0.000$ ), resulting in the rejection of the null hypothesis ( $H_{02}$ ). This finding corroborates the observations of Cele, Adesanya, and Bello (2024), who reported that cyber fraud in e-banking services negatively affects customer loyalty and satisfaction. Aderinto (2025) further emphasized that banks suffering losses due to online banking fraud experience a decline in both financial performance and public confidence. The results indicate that when customers perceive online banking systems as vulnerable to fraud, they are less likely to engage with these platforms, potentially slowing the progress of digital financial inclusion in Nigeria.

**4.4 Policy Implications of Findings**

The findings of this study carry significant implications for policy formulation and implementation in the Nigerian banking sector. Firstly, the demonstrated negative effect of phishing and online banking fraud on customer trust suggests that regulatory agencies such as the Central Bank of Nigeria (CBN) and the Nigeria Deposit Insurance Corporation (NDIC) need to enforce stricter cybersecurity standards for all deposit money banks. Policies mandating regular cybersecurity audits, penetration testing, and implementation of anti-phishing mechanisms would reduce the incidence of cyber fraud and enhance customer confidence.

Secondly, the study highlights the importance of integrating digital forensic practices into bank operations. Policymakers could introduce regulations requiring banks to maintain forensic investigation units capable of tracing cyber fraud, recovering funds, and providing evidence for legal action. Such policies would reinforce the accountability and transparency of financial institutions, thereby restoring and sustaining customer trust.

Thirdly, the findings suggest that customer education and awareness programs should be a regulatory requirement. Banks need policies to ensure that customers are regularly informed about potential cyber threats, safe online banking practices, and mechanisms for reporting fraud. Educated customers are less likely to fall victim to phishing and online banking scams, which in turn strengthens overall trust in the banking system.

**5.0 Conclusion and Recommendation**

The study examined the effect of cyber fraud on customer trust in Nigerian deposit money banks, focusing specifically on phishing and online banking fraud. The analysis revealed two major findings. First, phishing was found to have a significant negative effect on customer trust. Customers who experienced or were aware of phishing attacks showed reduced confidence in the safety and reliability of online banking platforms. This indicates that phishing, by exploiting vulnerabilities in digital interactions, directly undermines customers' willingness to engage

with electronic banking services. Second, online banking fraud was also shown to significantly decrease customer trust. Incidents of unauthorized transactions or fraudulent activities in online banking caused customers to question the competence and integrity of the banks in safeguarding their funds. Even customers who had not been directly affected expressed concerns over the security of digital banking systems when such frauds are reported or experienced by others.

The study investigated the effect of cyber fraud on customer trust in Nigerian deposit money banks, focusing on phishing and online banking fraud from a digital forensic perspective. The findings indicate that both forms of cyber fraud significantly erode customer trust. Phishing undermines confidence by exploiting vulnerabilities in digital interactions, while online banking fraud raises doubts about the banks' ability to safeguard funds and maintain secure platforms.

These findings underscore the critical importance of robust cybersecurity and digital forensic practices. Banks must not only prevent cyber fraud but also actively detect, trace, and resolve incidents to restore and maintain customer trust. In essence, the study concludes that customer confidence in digital banking systems is highly sensitive to cyber threats, and proactive measures particularly the integration of forensic capabilities are essential to sustain trust and encourage the continued adoption of online banking services in Nigeria.

- i. Banks should implement robust anti-phishing strategies, including advanced email filters, two-factor authentication, and real-time alert systems, to protect customers from fraudulent communications. Additionally, banks should conduct regular customer education programs to raise awareness about phishing tactics and safe online banking practices. These measures will help reduce the negative impact of phishing on customer trust.
- ii. To address the threat of online banking fraud, banks should invest in secure transaction monitoring systems and establish dedicated digital forensic units. These units should focus on detecting, tracing, and resolving fraudulent activities promptly. By demonstrating the ability to investigate and recover from fraud, banks can restore customer confidence and reinforce trust in their digital platforms.

## REFERENCES

- Adeniran, T. M., & Abiola, A. O. (2022). Cybercrime and financial stability in Nigerian banking institutions: An empirical assessment of digital risks. *Journal of Banking Security and Risk Management*, 8(2), 45–59.
- Aderinto, T. O. (2025). *The effect of cybersecurity threats on the financial performance of listed commercial banks in Nigeria*. *International Journal of Banking and Finance Research*, 12(2), 45–60.
- Ajayi, F. I., Oloyede, J. A., & Adejayan, A. O. (2021). Electronic bank fraud in Nigeria: The need to enhance customers' trust. *American Based Research Journal*, 10(4). Retrieved from <https://www.abri.org/publications-of-abri/article/595/?download=>
- Alsayed, A., & Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*, 7(1), 109-115.
- BusinessDay. (2025, March 31). E-fraud and digital banking security. *BusinessDay Nigeria*. Retrieved from <https://businessday.ng/opinion/article/e-fraud-and-digital-banking-security>.
- Cele, P., Adesanya, L., & Bello, M. (2024). *Cybersecurity threats and e-banking service delivery in Nigeria: Implications for customer trust and loyalty*. *African Journal of Digital Finance*, 5(2), 78–95.
- Eze, C. U., & Ekwueme, S. C. (2023). Online fraud and the erosion of customer confidence in Nigeria's digital banking system. *African Journal of Finance and Digital Economy*, 11(4), 101–118.
- Hasan, N., Khan, R., & Ibrahim, F. (2023). Cybersecurity awareness and data protection practices in emerging economies: Evidence from Sub-Saharan Africa. *International Review of Information Systems and Security*.
- Hasan, M. M., Siam, S. A. J., & Haque, A. (2023). The significance of customer service in establishing trust and enhancing the reputation of the banking industry in Bangladesh. *Business and Economics in Developing Countries*, 1(2), 47-51.
- Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, 26(2), 107.
- Mondaq. (2024). *Leveraging digital forensics to mitigate the risk of financial fraud [White-collar crime, anti-corruption & fraud analysis]*. Retrieved from

<https://www.mondaq.com/nigeria/white-collar-crime-anti-corruption-fraud/1373430/leveraging-digital-forensics-to-mitigate-the-risk-of-financial-fraud>

- Oloyede, F. I., Akinyele, S. T., & Adejayan, A. O. (2021). *Electronic bank fraud in Nigeria: The need to enhance customers' trust*. *American Based Research Journal*, 10(4), 15–32.
- Onamusi, G. E., Farouk, M. A., Uyagu, B. D., & Ekele, J. S. (2024). *Effect of digital forensic accounting technological tools on cyber financial fraud detection among quoted deposit money banks in Nigeria*. *International Journal of Capacity Building in Education and Management*, 6(5), 45-57.
- Oyibo, O. P., & Ifatimehin, O. O. (2024). Assessing the Impact of Cybersecurity Threats on E-Banking Adoption in Nigeria: A Study of Consumer Behaviour and Perception. *ASRIC Journal of Social Sciences*, 5(2).
- Reuters. (2025, September 16). Microsoft seizes 340 websites linked to growing phishing subscription service. *Reuters*. Retrieved from <https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-seizes-340-websites-linked-growing-phishing-subscription-service-2025-09-16/>
- Ripples Nigeria. (2023, June). Feature: Cyber fraud erodes Nigerians' faith in digital banking. *Ripples Nigeria*.
- Soetan, T. O., & Mogaji, E. (2024). Modernization of the Nigerian Financial System. In *Financial Services in Nigeria: The Path Towards Financial Inclusion, Economic Development and Sustainable Growth* (pp. 245-268). Cham: Springer Nature Switzerland.
- Umoh, E., Obaje, D., & Eze, P. (2024). *Bank fraud, public trust, and economic stability in Nigeria*. *Nigerian Journal of Financial Crime Studies*, 8(1), 23–41.
- Wang, H., Zhang, Y., & Li, X. (2020). *Cyber-dependent crimes and internet banking security in emerging economies: Evidence from Nigeria*. *Journal of Financial Crime*, 27(3), 987–1005.