IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM

[1]Timothy Abayomi ATOYEBI, Ph.D., [1]Abdulkadir USMAN, [1]Cosmas VICTOR, [2]Ikoh Samson JOSEPH and [1]Edime YUNUSA*

[1]Department of Sociology, Faculty of Social Sciences, Prince Abubakar Audu University, Anyigba, Kogi State - Nigeria

[2]Department of Public Administration, Faculty of Management Sciences, University of Abuja– Nigeria

Abstract

The expansion of digital banking has transformed financial service delivery while simultaneously increasing exposure to cyber-related threats within the Nigerian banking system, making bank security a growing concern for regulators, institutions, and customers. This paper examined cybercrime and financial institutions by reviewing bank security in Nigeria with the objective of analysing how cybercriminals gain access to individual and corporate accounts, why cybercrime persists despite regulatory interventions, the socio-economic implications for the banking sector and national image, and the effectiveness of institutional and customer responses to cyber crime. The paper was anchored on Routine Activity Theory, which explains cybercrime as a function of the convergence of motivated offenders, suitable targets, and weak guardianship within routine digital banking activities. Adopting a theoretical and systematic review methodology, the paper relied exclusively on secondary data drawn from peer-reviewed academic studies, regulatory publications, and industry reports relevant to cybercrime and banking operations in Nigeria. The paper showed that cybercrime is facilitated by social engineering techniques, technological gaps, insider collaboration, and uneven digital literacy, while unemployment, inequality, and weak enforcement sustain offender motivation. The paper further revealed that cybercrime imposes financial losses, undermines trust in digital banking, and damages Nigeria's domestic and international reputation. Although banks and customers have adopted security measures, these responses remain uneven and largely reactive. The paper concluded that strengthening institutional guardianship is central to improving bank security. It therefore recommended enhanced technological controls, stronger regulatory coordination, sustained cybersecurity education, and integrated socio-economic interventions to reduce cybercrime risks in Nigeria's banking sector.

KEYWORDS: Cyber Crime, Bank Security, Financial Institutions, Cybersecurity, Digital Banking Nigeria

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Introduction

Over the past decade, the banking sector in Nigeria has undergone rapid digital transformation as financial institutions adopt online and mobile banking platforms, electronic payment systems, and networked information systems to enhance service delivery and operational efficiency. This shift has markedly increased the sector's exposure to cyber threats, as cybercriminals exploit vulnerabilities inherent in digital infrastructures. Empirical studies have documented a significant escalation in cyber attacks on Nigerian financial institutions; for instance, a 2024 report by Check Point Software Technologies revealed that Nigerian banks faced 182 % more weekly cyberattacks compared with global peers, with threats such as InfoStealer and banking trojans targeting key systems (Jaiyeola, 2024).

Such attacks have tangible financial impacts: fraud related losses reported by the Nigeria Inter-Bank Settlement System exceeded tens of billions of naira in recent periods, and the Financial Institutions Training Centre noted sharp increases in fraud losses between 2023 and 2024 (Jaiyeola, 2024). Other evidence points to broader economic consequences, with the National Bureau of Statistics and the National Information Technology Development Agency reporting annual national losses attributable to cybercrime in the hundreds of billions of naira, often linked to account takeovers and SIM-swap fraud (Sambo, 2025).

Academic investigations corroborate these trends within the Nigerian context. For example, research by Ama et al. (2024) identifies pharming, identity theft, and SIM swap fraud as prominent cybersecurity challenges confronting deposit money banks, while other studies highlight phishing, skimming, malware, and denial-of-service incidents as recurring threats that undermine banks' performance and operational continuity (Okpa, 2024). The cumulative effect of such cyber risks undermines public confidence, erodes financial stability, and imposes substantial costs on institutions that must invest in detection, prevention, and remediation capabilities. At the same time, criticisms have arisen regarding the adequacy and strategic alignment of cybersecurity investments by major banks; despite billions of naira allocated to technology budgets, questions persist about whether existing spending sufficiently addresses evolving threat landscapes (Jaiyeola, 2024). These dynamics point to urgent needs for both empirical assessment and policy-oriented inquiry into bank security practices, regulatory

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

frameworks, and institutional responses to cybercrime in Nigeria. Hence, the paper examined Cyber crime and financial institutions with specific focus on banks security in Nigeria.

Statement of the Problem

Despite the recognized importance of digital banking for financial inclusion and economic growth in Nigeria, rising incidents of cybercrime pose a serious threat to the security of financial institutions and the integrity of the national financial system. Nigerian banks are disproportionately targeted by cyberattacks compared to global averages, resulting in significant financial losses for both institutions and customers, and undermining confidence in electronic financial services (Jaiyeola, 2024; Sambo, 2025). While banks have increased their technology investment portfolios in recent years, there is concern that cybersecurity expenditures are insufficient or misaligned with the nature and sophistication of emerging threats, leaving vulnerabilities in critical infrastructure and fraud controls (Jaiyeola, 2024). Empirical studies have identified a range of specific cybercrime modalities such as phishing, skimming, malware, SIM swap fraud, and identity theft that continue to erode operational effectiveness and performance in deposit money banks, suggesting gaps in both preventive and responsive security measures (Ama et al., 2024; Okpa, 2024).

Moreover, there is limited consensus in the literature regarding the effectiveness of current security frameworks, the role of internal controls, and the adequacy of institutional collaboration with national cybersecurity agencies in mitigating risks. This gap is compounded by incomplete data on the incidence and impact of cybercrime within the Nigerian banking sector, which restricts policy-makers' and practitioners' ability to formulate evidence-based responses. Without a rigorous review of bank security practices and the cyber threat environment specific to Nigeria, financial institutions may remain exposed to evolving threats, potentially leading to further financial losses, regulatory sanctions, and deterioration of public trust in digital financial services. Therefore, it is crucial to systematically examine the extent to which cybercrime affects bank security in Nigeria and to identify the structural, technological, and regulatory factors that impede effective mitigation.

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Aim and Objectives of the Paper

The aim of this paper was to examine cyber crimes and financial institutions. A review of banks security in Nigeria. The specific objectives were to;

i. examine the various ways through which cybercriminals gain unauthorised access to individual and corporate bank accounts in Nigeria.
ii. analyse the factors responsible for the persistence of cybercrime in Nigeria despite existing legislative and regulatory measures.
iii. assess the socio-economic implications of cybercrime on Nigerian financial institutions and the country's image at the domestic and international levels.
iv. evaluate the security measures adopted by banks and other corporate organisations in Nigeria to prevent and mitigate cybercrime.
v. examine how bank customers in Nigeria have responded to and overcome the challenges posed by cybercrime in digital banking transactions.

Literature Review

The literature were reviewed in line with the aim and objectives of the paper under conceptual review, empirical review and theoretical framework.

Conceptual Review

The key concepts in this paper are reviewed as follows:

Cyber Crime

The term cyber crime literally refers to offences committed through the use of information and communication technologies that violate legal norms and cause harm to systems, data, or individuals. While there is no universally agreed definition among scholars, most definitions underscore the role of digital technologies in the commission of illegal acts. The European Parliamentary Research Service (2024) describes cyber crime as acts that use information technology to perpetrate or facilitate a crime, distinguishing between "cyber-dependent"

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

offences, those that can only be committed using ICT and "cyber-enabled" offences, traditional crimes facilitated by digital technologies.

This distinction is echoed in academic analyses, which note that cyber crime covers a spectrum of harmful behaviours ranging from hacking, malware deployment, and ransomware, to fraud and identity theft conducted via online networks (United Nations Office on Drugs and Crime, 2024). Classic encyclopaedia sources similarly define cyber crime as using a computer as an instrument to further illegal ends such as fraud, theft, or privacy invasion, emphasising the centrality of the networked digital environment to the offence (Encyclopaedia Britannica, 2025).

These scholarly views highlight that cyber crime is not limited to a single offence but is an evolving set of illegal acts shaped by technological change. For the purpose of this paper, cyber crime is defined as any unlawful act committed with the assistance of information and communication technologies, where computer networks, digital systems, or internet-based tools are integral to the execution or facilitation of the offence.

Financial Institutions

Financial institutions are formal organisations authorised to carry out financial intermediation and related services, serving as essential components of the monetary and economic system. Legal and regulatory frameworks, such as the Nigerian Cybercrimes Act 2015, explicitly recognise financial institutions to include banks, insurance firms, investment companies, and other entities engaged in financial intermediation, payments, securities, and exchange services (Nigeria Cybercrimes Act 2015).

Scholarly and institutional definitions generally describe financial institutions as entities that mobilise savings, provide credit, offer payment and settlement services, and manage financial risk for individuals, corporations, and governments. Such institutions are inherently custodians of monetary assets and sensitive financial information; their role in economic stability and public confidence underscores their vulnerability to threats in cyberspace (FDIC, 2025).

The literature on cyber threats targeting the financial sector emphasises that because financial institutions manage critical economic infrastructure, they are prominent targets for cyber criminals seeking monetary gain or disruption (Darktrace, 2025). In this paper, financial

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

institutions refer to legally authorised entities, including banks, deposit-taking organisations, and other regulated financial service providers, whose core functions include managing financial assets, facilitating payments, and providing credit and investment services within the economic system.

Bank Security

Bank security in the scholarly domain encompasses the range of measures deployed by banks to protect their information systems, customers, assets, and operational processes against threats that could compromise integrity, confidentiality, or availability. While definitions vary, bank security is often discussed in the context of protecting physical and digital assets from criminal activity, fraud, and external attacks. In the specific context of cyber threats, bank security includes technical controls, procedural safeguards, and organisational practices that mitigate risk to banking systems and customer data (Oyewole et al., 2024).

Research focused on the banking sector in Nigeria highlights that cybersecurity deficits or inadequate security measures correlate with increased incidences of fraud such as ATM scams, phishing, and account takeovers demonstrating the operational implications of weak security postures (Oyewole et al., 2024). The literature suggests that bank security is not strictly limited to reactive tools; it also comprises proactive detection, incident response, and risk management strategies tailored to the digital threat environment per se.

For this paper, bank security is defined as the complete suite of protective measures such as technical, procedural, and managerial that a bank employs to safeguard its systems, data, customers, and operations against criminal activity and security breaches.

Cyber Security

Cyber security literally denotes the organised practices, technologies, and governance mechanisms designed to defend information systems and networks from unauthorised access, damage, or disruption. Scholarly sources highlight that cybersecurity involves identifying, preventing, detecting, and responding to threats against digital infrastructure. Because financial systems increasingly depend on digital communications and interconnected networks,

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

cybersecurity practices have become central to maintaining operational continuity and trust (Waliullah et al., 2025).

Academic definitions emphasise that cyber security is not merely a technical discipline but also includes risk assessment, governance frameworks, and response capabilities that work jointly to preserve the integrity of information systems against attacks such as malware, phishing, and data breaches. In the context of banking and financial institutions, cyber security extends to the protection of customer credentials, online transaction platforms, backend servers and communication channels against cyber threats (Waliullah et al., 2025).

Therefore, for the purposes of this paper, cyber security is adopted as the organised application of practices, technologies, policies, and processes designed to protect networked information systems and digital assets from unauthorized access, harm, or exploitation

How Cyber Criminals Have Access to Bank Accounts (Individual and Corporate) in Nigeria

There are many ways through which cyber criminals gain access to individuals and Coperate bank accounts, some of which are identified and discussed as follows:

i. Social Engineering and Pitching

One of the primary avenues through which cyber criminals gain access to bank accounts in Nigeria is social engineering**,** a technique that manipulates users into divulging confidential information. Fraudsters commonly deploy phishing attacks on emails or SMS messages that mimic legitimate bank communications to trick users into entering their login credentials or OTPs on fake banking portals (Okafor & Ugbaja, 2025). Empirical data indicate that phishing attacks have surged markedly alongside digital banking adoption; between 2022 and 2023, phishing incidents nearly tripled, with corresponding financial losses rising from ₦240.6 million to ₦551.2 million, illustrating the scale and growth of this threat vector in Nigeria's banking context (Okafor & Ugbaja, 2025).

ii. Identity Theft

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Closely related to phishing is identity theft, where fraudsters harvest personal data such as BVN, passwords, or personal details via malicious apps or unsecured public Wi-Fi networks (Ngwu et al., 2025). Once obtained, these credentials enable unauthorized login to online and mobile banking platforms. Studies suggest that Bank Verification Number (BVN) scams, where attackers trick customers into revealing their BVN and OTPs, facilitate unauthorized access and subsequent theft, undermining trust and inhibiting banking system growth (Ngwu et al., 2025). Moreover, ATM skimming devices, which intercept card details and PINs at ATMs or point-of-sale terminals, remain a significant physical-to-digital conduit for attacks in urban Nigerian settings, particularly in areas with high foot traffic.

iii. SIM Swap Fraud

Another sophisticated mode of unauthorized access is SIM swap fraud, where attackers deceive mobile network operators into transferring a victim's phone number to a SIM card controlled by the criminal. With control of the victim's phone number, attackers can receive OTPs necessary for two-factor authentication and execute unauthorized transfers (Mustapha & Sinha, 2024). According to these authors, industry reports and cyber risk assessments highlight this method as a persistent and expensive threat, particularly given Nigeria's high mobile penetration and reliance on SMS-based authentication.

iv. Malware and Credential-Harvesting

Malware and credential-harvesting tools also provide entry points into bank accounts. Malicious software deployed via infected email attachments or compromised apps can log keystrokes, capture screen information, or siphon session tokens without user awareness. Ama et al. (2024) note that banking systems are regularly targeted by malware and ransomware attacks that compromise back-end systems and customer data (Ama et al., 2024). These technical exploits often bypass superficial security controls when coupled with poor encryption or delayed patching.

v. Insider Collusion and Weak Internal Controls

Moreover, insider collusion and weak internal controls within banks themselves have been implicated in breaches. An analysis of cybersecurity challenges in Nigerian banks underscores

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

that insufficient automatic logout policies, inadequate security audits, and collusion between staff and external criminals exacerbate vulnerability (Adeyemi, 2025). This author admits that in corporate accounts, particularly where multiple signatories and privileged access exist, malicious insiders or poorly monitored access rights can facilitate unauthorized transfers with little immediate detection. Collectively, these diverse attack vectors demonstrate that cybercriminals exploit both human and technical weaknesses to access individual and corporate bank accounts in Nigeria.

Why Cyber Crimes Thrive Despite Legislative and Regulatory Measures

Despite the implementation of legislative frameworks like Nigeria's Cyber Crimes Prohibition, Prevention Act, cyber crime continues to proliferate, driven by a combination of socio-economic, technological, and enforcement challenges. One fundamental driver is economic hardship, including high unemployment and pervasive poverty, which create incentives for some individuals especially youths with digital literacy but limited job opportunities to engage in illicit cyber activities. Research on socioeconomic determinants of cybercrime reveals that lack of formal employment and income inequality correlate strongly with increased cyber offending, suggesting structural conditions significantly facilitate cybercrime (Aneke et al., 2025).

Another crucial factor is the rapid growth in digital banking adoption without commensurate cyber security awareness and capacity among users and institutions alike. While awareness studies show that many Nigerian banking customers recognize cybercrime risks, gaps remain in secure password practices and holistic understanding of threat vectors, meaning user behaviours still expose systems to compromise (Garba et al., 2023). Furthermore, infrastructure challenges such as outdated systems, insufficient multi-factor authentication coverage, and legacy software—leave exploitable openings that legislation alone cannot patch.

Legislative and enforcement deficits also play a significant role. Although Nigeria has laws targeting cyber offences, enforcement is often hindered by limited specialized personnel, inadequate forensic capacity, and slow prosecution processes, leading to low conviction rates relative to the number of reported incidents. Studies of financial crime enforcement note that even when agencies like the Economic and Financial Crimes Commission investigate cyber

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

fraud, evidentiary requirements and technical complexities often result in protracted cases with few conclusive outcomes (Ogunmokun, 2024). These institutional weaknesses diminish the perceived risk of prosecution among potential offenders.

The digital ecosystem itself characterised by high mobile and internet penetration has outpaced regulatory adaptation, meaning new threat techniques such as advanced phishing, social engineering, and malware automation evolve faster than regulatory safeguards. Digital financial services, including mobile banking and fintech payment apps, often operate at the frontier of regulation, with cyber security mandates lagging behind innovation cycles. As a result, cybercriminals exploit gaps in real-time monitoring, anomaly detection, and mandated reporting requirements (Garba et al., 2023).

Moreover, weak collaboration mechanisms between banks, telecom operators, and law enforcement further enable cybercrime. Effective cyber deterrence requires real-time information sharing and coordinated response protocols, yet siloed data governance and privacy concerns limit these collaborations. Without integrated public-private partnerships that align regulatory oversight with operational threat intelligence, breaches are addressed reactively rather than prevented pre-emptively (Ogunmokun, 2024).

Thus, a combination of socio-economic conditions, technological gaps, enforcement limitations, and collaborative shortfalls explain why cybercrime persists despite Nigeria's legislative and regulatory measures.

Socio-Economic Implications of Cyber Crimes on the Image of Nigeria

The socio-economic implications of cybercrime in Nigeria are expansive and extend beyond immediate financial losses to affect national reputation, investor confidence, and societal trust. A major consequence of cybercrime is the erosion of trust in digital financial systems, which undermines broader economic development goals such as financial inclusion and digital transformation. Research indicates that persistent cyber fraud deters segments of the population from adopting digital financial services, slowing the country's progress toward comprehensive financial inclusion and undermining confidence in electronic payment systems (Darktrace. (2025).

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Economically, direct losses from cybercrime affect both individuals and institutions. Data from national surveys show that Nigerian consumers and banks collectively lose billions of naira annually due to hacking, identity theft, and other cyberattacks, thus diverting financial resources away from productive investment and into remediation and risk mitigation efforts. These losses strain household budgets and corporate balance sheets alike, reducing disposable income, inhibiting investment, and increasing the cost of banking services as institutions attempt to recoup security-related expenditures (Ngwu et al., 2025). The allocation of resources toward reactive cybersecurity measures also diverts public and private funds from sectors such as education, health, and infrastructure.

Beyond financial metrics, cybercrime impacts Nigeria's national brand and foreign investment climate. Global investors increasingly assess digital risk environments as part of due diligence; a high incidence of cyber fraud communicates vulnerability and operational risk that can deter foreign direct investment (Adeyemi, 2025). International partners may perceive Nigeria as a high-risk environment for technology and financial services, potentially limiting bilateral cooperation, outsourcing opportunities, or entry of international fintech firms. Such perceptions have reputational consequences that extend into Nigeria's broader economic engagements.

At the societal level, Mustapha and Sinha (2024) posit that cyber crime can exacerbate social inequality and distrust, particularly when high-profile breaches disproportionately affect vulnerable populations with less capacity to recover losses. Rural and underserved communities, where digital literacy may be lower and access to redress mechanisms more constrained, often suffer greater long-term harm reducing confidence in formal financial institutions and pushing individuals toward informal or cash-based systems that are less efficient and secure.

Finally, significant cybercrime rates contribute to negative international narratives about Nigeria's regulatory effectiveness and security posture. International media and cybersecurity reports highlighting Nigerian origins of certain syndicates (e.g., SilverTerrier) influence global perceptions, sometimes unfairly conflating criminal activity with broader national characteristics (Njidofor et al., 2025). While law enforcement agencies such as the Economic and Financial Crimes Commission work to address cyber fraud, persistent incidents risk reinforcing stereotypes that harm national dignity and global cooperative efforts.

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Security Measures Put in Place by Banks to Overcome Cyber Crime in Nigeria

In response to the rising incidence of cyber crime, Nigerian banks and corporate organisations have adopted a range of technical, procedural, and strategic security measures designed to enhance resilience and protect customers.

One of the most obvious measures identified by Abba et al. (2025) is multi-factor authentication (MFA), which requires customers to verify their identity using two or more credentials such as a password plus an OTP or biometric factor before accessing accounts or approving transactions. The Central Bank of Nigeria's risk-based cybersecurity guidelines notably promote MFA as a baseline control for deposit money banks and payment service providers.

Banks also deploy advanced encryption protocols to secure data in transit and at rest, reducing the risk of interception or unauthorized access. Encryption technologies ensure that even if data are captured through network sniffing or phishing, they remain unintelligible without decryption keys, thereby reducing the usable value of stolen information (Sunday et al., 2025). Additionally, many institutions invest in real-time anomaly detection and fraud monitoring systems, which analyse transaction patterns for irregular activities and flag or block suspicious behaviour. These systems employ machine learning and rule-based triggers to identify potential breaches enhancing detection speed and reducing customer impact (Okpa, 2024).

Security awareness and customer education initiatives constitute another critical layer of defence. Banks conduct campaigns to educate customers on the dangers of phishing, strong password practices, avoiding unsecured Wi-Fi, and recognising fraudulent communications. Awareness studies reveal that a significant portion of Nigerian online banking users are aware of cybercrime risks, which supports the effectiveness of sustained education efforts, although gaps remain (Garba et al., 2023). These initiatives help reduce the human error vector, which is often the initial breach point in fraud schemes.

Internally, organisations implement regular security audits, vulnerability assessments, and penetration testing to identify and remediate weaknesses in their networks, applications, and databases. These periodic evaluations help ensure that systems remain patched against known vulnerabilities and that new threat signatures are incorporated into defensive controls. In some

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

cases, firms also engage in third-party threat intelligence sharing and collaborate with industry forums like the Nigeria Electronic Fraud Forum (NeFF) to exchange information about emerging threats and collectively improve detection strategies (CBN Risk-based Framework, 2024).

Finally, Sunday et al. (2025) note that strategic governance and risk management frameworks guide organisational approaches to cybersecurity. Boards and executive leadership increasingly view cybersecurity as a strategic risk, embedding cyber incident response planning, disaster recovery, and business continuity protocols into enterprise risk management. While gaps persist, these structured approaches demonstrate progress toward a more holistic security posture that integrates people, process, and technology.

Bank Customers and the Challenges of Cyber Crime in Nigeria

Bank customers in Nigeria have adopted various personal and technological strategies to mitigate the risks of cybercrime and protect their financial assets. A common customer response is the use of multi-factor authentication and strong authentication practices, such as combining robust passwords with biometric logins or unique OTPs, which significantly reduce the likelihood of unauthorized access via stolen credentials. Industry advice emphasises these practices as foundational to securing online accounts (Owolabi, 2024).

Customers have also increased vigilance and self-monitoring, regularly checking account statements and transaction histories for unusual activity. This proactive behaviour enables rapid detection of suspicious transactions, allowing customers to report issues to their banks for immediate action, such as freezing accounts or reversing fraudulent transfers. While not all fraud is reversible, early detection mitigates the scale of losses and engages institutional investigation mechanisms more effectively (Owolabi, 2024).

Education and awareness have played a critical role in preparing customers to recognise and avoid common fraud vectors, such as phishing emails, unsolicited calls requesting personal details, or links leading to fraudulent banking portals. Customers who understand the tell-tale signs of scams are less likely to fall victim to social engineering. Awareness campaigns by banks and industry groups have contributed to this improved understanding, although gaps in secure behaviour remain an ongoing challenge (Garba et al., 2023).

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

In some cases, customers adopt enhanced security tools such as password managers to ensure unique and complex credentials across platforms, virtual private networks (VPNs) to secure connections on public Wi-Fi, and dedicated security software on their devices to reduce malware exposure (Waliullah et al., 2025). These tools add logistical hurdles for attackers and help safeguard sensitive information from interception.

Finally, customers increasingly leverage reporting mechanisms and redress channels, including bank hotlines, online fraud reporting portals, and law enforcement cybercrime units like those under the Economic and Financial Crimes Commission (EFCC). Reporting fraud promptly triggers institutional support mechanisms and increases the likelihood that fraudulent transactions will be investigated and contained (Economic and Financial Crimes Commission, 2024). While systemic challenges in prosecution remain, customer engagement with formal reporting helps build evidence against criminals and contributes to broader deterrence efforts.

Empirical Review

Empirical studies abound on the subject matter of this paper, among the relevant ones are reviewed as follows:

Njidofor et al. (2025) examined the influence of specific cyber crime modalities on the sustainable development of deposit money banks in Enugu State, Nigeria. Anchored on implicit risk theory, the study adopted a descriptive survey design to explore how ATM skimming and phishing undermine institutional development. Data were collected using structured questionnaires administered to a sample of 371 bank users drawn from a total population of 773,000 via the Freund and Williams sampling technique. The questionnaire captured respondents' experiences and perceptions of cyber crime incidents affecting their banks. Statistical analysis using frequency, mean, standard deviation, and regression models revealed that both ATM skimming and phishing scams had statistically significant negative effects on bank sustainability (t-statistics: –8.954 and –6.491, respectively, $p < .05$), reflecting how cybercriminal exploits erode depositor confidence, distort operational continuity, and disrupt strategic objectives in banking institutions. The authors concluded that cyber crime constitutes a substantial barrier to sustainable banking development and recommend robust identity systems

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

and centralized databases to support fraud detection. While this study provides valuable localized insight, its reliance on self-reported perceptions limits generalisability across different geo-economic regions of Nigeria and does not unpack mechanisms banks use to mitigate these effects in practice, a gap the current paper addressed by systemat and theoretically assessing institutional responses and security architectures across multiple Nigerian financial zones.

In a more comprehensive empirical analysis, Okafor (2025) investigated the linkage between the adoption of online banking services and the incidence of phishing and online scams throughout Nigeria's financial sector. The study covered 2020–2024 panel data spanning national fraud datasets (from NIBSS, CBN, NCC, and EFCC) and integrates secondary sources including industry and international reports to establish trends. The research rested on the routine activity theory, which posits that increased digital activity creates more opportunities for motivated offenders. Using an instrumental variable estimation technique, the study quantitatively models the relationship between digital banking penetration and cybercrime using secondary data rather than primary survey responses, preserving analytical rigor in addressing endogeneity concerns. Findings indicated a strong positive correlation between online banking adoption and cybercrime incidents: phishing attacks nearly tripled from 1,667 cases in 2022 to 4,457 in 2023, with reported associated financial losses growing from ₦240.6 million to ₦551.2 million. A 10 % increase in digital banking uptake was statistically associated with a 3.42 % increase in cybercrime occurrences, signifying the dual-edged nature of financial innovation in emerging economies such as Nigeria. The study concluded that while digital adoption expands financial inclusion, it simultaneously amplifies opportunities for fraud, necessitating nuanced policy intervention targeting the cybercrime-digitalisation nexus. The limitations here include a lack of qualitative insights into organisational cyber security practices and individual customer behaviour in fraud mitigation, which the current paper investigated.

Abba et al. (2025) explored how cybersecurity practices affect organisational network resilience within selected commercial banks in Nigeria, guided by the Technology-Organisation-Environment (TOE) theory, which posits that technological, organisational, and environmental contexts influence security adoption and performance outcomes. Using a descriptive survey design, the researchers administered structured questionnaires to 192 IT employees across

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

multiple commercial banks, selected via a multi-stage sampling technique. Data analysis employed frequency distributions, percentages, and Likert scales to interpret perceptions of cyber threats and their implications for network integrity. Results revealed that cyber attacks on banks' networked systems occur at high frequency and deeply influence operational digitalisation trajectories, data protection priorities, and collaborative security responses. Specifically, respondents indicated that recurring attacks stimulated improvements in digital operational protocols, enhanced customer data protection efforts, and strengthened organisational appreciation for synergy among cybersecurity stakeholders. The authors concluded that while cyber threats are pervasive, they serve as catalysts for advancing robust security postures within banks highlighting a potential positive externality of exposure to threats. Importantly, this study's IT employee-centric perspective omits frontline managerial, regulatory, and customer viewpoints, creating a gap for broader multi-stakeholder analysis that the current paper provided, especially with attention to cross-sectoral implications and coordinated defence strategies beyond internal IT functions.

Theoretical Framework: Routine Activity Theory (RAT)

Routine Activity Theory was proposed by Lawrence E. Cohen and Marcus Felson in 1979 in their seminal work on social change and crime rates. The theory was developed to explain variations in crime occurrence not by offender motivation alone but by changes in everyday activities that create opportunities for crime. Cohen and Felson argued that crime is likely to occur when three essential elements converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian. Their formulation shifted criminological focus away from offender pathology toward situational conditions that enable criminal acts.

The major assumption of Routine Activity Theory is that criminal behaviour is largely opportunistic and influenced by environmental and situational factors rather than solely by individual dispositions. The theory assumes that motivated offenders exist in society at all times; therefore, fluctuations in crime rates are better explained by changes in target suitability and guardianship. It also assumes that technological and social transformations alter routine patterns of interaction, thereby reshaping crime opportunities. In modern applications, scholars extend the notion of "space" beyond physical environments to include virtual spaces, recognising that

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||

online platforms and digital systems function as routine activity settings where crime can occur when protective controls are weak.

The strengths of Routine Activity Theory lie in its flexibility and adaptability to contemporary forms of crime, including cybercrime. The framework has been widely applied in empirical studies on online fraud, identity theft, and financial cybercrime because it explains how increased internet use, mobile banking, and digital payment systems expand the pool of suitable targets while simultaneously weakening traditional guardianship mechanisms. Another strength is its policy relevance: by focusing on guardianship, the theory directly informs preventive strategies such as strengthening security controls, improving surveillance systems, and enhancing user awareness. However, the theory is not without weaknesses. Critics argue that it downplays broader structural and socio-economic drivers of crime, such as inequality and unemployment, by assuming offender motivation as constant. Additionally, it offers limited insight into why certain individuals become motivated offenders in the first place, focusing instead on the circumstances that enable criminal acts.

The relevance of Routine Activity Theory to the present study is particularly strong within the Nigerian banking context. The rapid expansion of digital banking services, mobile money platforms, and electronic payment systems has significantly altered routine financial activities, increasing customers' exposure to cyberspace. Nigerian banks and their customers constitute highly suitable targets due to the concentration of financial assets and sensitive personal data within interconnected systems. At the same time, gaps in cyber security infrastructure, insider collusion, low digital literacy among segments of the population, and delayed regulatory enforcement represent weakened guardianship. Motivated offenders both domestic and transnational exploit these conditions through phishing, SIM-swap fraud, malware attacks, and account takeovers.

By applying Routine Activity Theory, this paper was able to systematically explain how the convergence of offender motivation, target suitability, and insufficient guardianship produces persistent cybercrime risks in Nigerian financial institutions. The theory therefore provides a clear conceptual foundation for analysing bank security failures and for proposing preventive measures centred on strengthening institutional and technological guardianship mechanisms.

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Methodology

This paper adopted a theoretical and systematic review methodology which relied exclusively on secondary data to examine cybercrime and bank security within Nigerian financial institutions. The paper systematically reviewed existing scholarly literature, regulatory documents, industry reports, and policy publications relevant to cyber crime, cyber security, and banking operations in Nigeria. Sources were identified through careful screening of peer-reviewed journals, official publications from regulatory bodies such as the Central Bank of Nigeria and the Nigeria Inter-Bank Settlement System, and credible reports from international and national cybersecurity organisations. Inclusion criteria were based on relevance to the research focus, methodological rigour, and publication recency, while materials lacking empirical or institutional credibility were excluded. The selected sources were critically analysed using qualitative content analysis to identify recurring themes, patterns, and gaps in existing knowledge relating to cyber threats, institutional security measures, regulatory effectiveness, and socio-economic implications. By synthesising theoretical perspectives and empirical evidence from prior studies, the methodology enabled a coherent assessment of the nature and dynamics of cybercrime in Nigeria's banking sector without primary data collection, ensuring analytical depth, conceptual clarity, and contextual relevance.

Discussions

This paper examined how cyber crime affects bank security in Nigeria, the factors sustaining its prevalence, the implications for financial institutions and the national image, and the effectiveness of responses by banks and customers.

The paper consistently showed that cyber criminal access to individual and corporate bank accounts is largely enabled through social engineering, SIM swap fraud, phishing, malware, and insider collaboration. Authors such as Ama et al. (2024) and Okafor et al. (2025) emphasise that technological vulnerabilities alone do not explain these breaches; rather, human behaviour and organisational weaknesses play decisive roles. This supports the view that Nigerian banks operate in an environment where routine digital interactions online banking logins, mobile authentication, and electronic transfers have become predictable activities that offenders exploit.

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

The findings therefore reinforce the argument that cybercrime in the banking sector is less about isolated system failures and more about systemic exposure created by everyday digital banking practices.

The persistence of cyber crime despite legislative and regulatory measures reflects deeper structural and institutional challenges highlighted across the reviewed studies. Scholars including Aneke et al. (2025) and Ogunmokun (2024) argue that unemployment, poverty, and inequality provide a steady supply of motivated offenders, while weak enforcement capacity reduces deterrence. This paper's synthesis confirms that although Nigeria possesses formal legal instruments such as the Cyber Crimes Act, gaps in implementation, inter-agency coordination, and technical capacity undermine their effectiveness. The literature further suggests that rapid technological advancement in banking has outpaced regulatory oversight, creating security gaps that cyber criminals exploit. These observations align with the objective of explaining why cyber crime thrives, demonstrating that legal frameworks alone are insufficient without corresponding socio-economic interventions and institutional strengthening.

The socio-economic implications discussed in the paper show convergence among authors on the reputational and developmental costs of cybercrime. Studies reviewed indicate that recurring cyber fraud erodes public trust in digital banking, discourages adoption of electronic financial services, and increases operational costs for banks, which are often passed on to customers. Internationally, authors cited in the paper note that persistent cybercrime contributes to negative risk perceptions about Nigeria, affecting foreign investment decisions and cross-border financial relationships. This discussion underscores that cybercrime is not merely a technical or financial issue but a broader socio-economic concern with implications for national credibility, economic growth, and financial inclusion objectives.

In examining security measures adopted by banks and corporate organisations, the reviewed literature revealed incremental progress rather than complete resolution. Authors such as Abba et al. (2025) and the Central Bank of Nigeria (2024) point to the adoption of multi-factor authentication, encryption, fraud monitoring systems, and staff training as evidence of institutional response. However, the discussion shows that these measures often remain reactive, introduced after significant losses have occurred. Similarly, customer-level adaptations such as

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

increased vigilance, use of authentication tools, and reporting mechanisms demonstrate growing awareness but also highlight uneven digital literacy across user groups. The findings therefore suggest that while both institutions and customers are adjusting to cyber risks, defensive practices remain inconsistent and unevenly enforced.

The theoretical framework adopted in this paper, Routine Activity Theory, provides strong explanatory support for the findings. The theory's core elements motivated offenders, suitable targets, and absence of capable guardians are clearly reflected in the Nigerian banking context. The reviewed evidence shows that motivated offenders are sustained by socio-economic pressures, banks and customers constitute attractive targets due to concentrated financial assets and routine digital transactions, and guardianship is weakened by technological gaps, insider collusion, and enforcement limitations. By grounding the discussion within this framework, the paper demonstrates that cybercrime against financial institutions emerges from predictable interactions within everyday banking routines rather than random anomalies. Consequently, the theory justifies the paper's conclusion that strengthening guardianship—through improved institutional controls, coordinated regulation, and enhanced user awareness—is central to improving bank security in Nigeria.

Conclusion

This paper examined cyber crime and bank security in Nigeria through a systematic review of theoretical and empirical literature, with emphasis on access mechanisms, sustaining factors, socio-economic implications, and existing countermeasures. The findings indicated that cyber crime against Nigerian financial institutions is largely driven by routine digital banking activities that expose both individual and corporate accounts to phishing, SIM-swap fraud, malware attacks, and insider-related vulnerabilities. Despite the presence of legislative and regulatory frameworks, weak enforcement capacity, socio-economic pressures, rapid technological expansion, and inconsistent security practices continue to undermine effective deterrence.

Cyber crime has consequently eroded public trust in digital banking, imposed significant financial and reputational costs on banks, and negatively influenced Nigeria's domestic and international image. The application of Routine Activity Theory confirms that cyber crime in the

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

banking sector thrives where motivated offenders converge with suitable digital targets in the absence of sufficiently robust guardianship. Strengthening institutional, technological, and human safeguards therefore remains central to improving bank security and reducing cybercrime risks in Nigeria.

Recommendations

Arising from the above conclusions, the paper put forth the following recommendations;

1. Financial institutions in Nigeria should strengthen technological guardianship by implementing uniform and mandatory advanced authentication systems, real-time fraud monitoring tools, and regular vulnerability assessments across all digital banking platforms to reduce opportunities for account compromise.
2. Regulatory authorities in Nigeria should enhance enforcement effectiveness by improving inter-agency collaboration among banks, telecom operators, and security agencies, while investing in specialised cyber forensic capacity to ensure timely investigation and prosecution of cyber crime cases.
3. Banks and regulators in Nigeria should expand sustained customer and staff cybersecurity education programmes focused on recognising social engineering tactics, secure digital behaviour, and timely reporting mechanisms, thereby reducing human-related vulnerabilities within routine banking activities.
4. Government policy responses should integrate cyber crime control with broader socio-economic interventions, particularly youth employment and digital skills development initiatives, to address the underlying conditions that sustain a pool of motivated offenders in the cyber domain.

REFERENCES

Abba, M. O., Osodeke, E. C., & Ibekwe, C. C. (2025). Effect of cyber security on organisation network: Evidence from selected commercial banks in Nigeria. *Contemporary Journal of Cyber Security,* 3(3), 103–118.

Adeyemi, A. (2025). The cost of cyber insecurity: How it affects Nigeria's digital economy. https://businessday.ng/opinion/article/the-cost-of-cyber-insecurity-how-it-affects-nigerias-digital-economy/

IJO -INTERNATIONAL JOURNAL OF BUSINESS MANAGEMENT
(E:ISSN 2811-2504) (P.ISSN: 2384-5961) Edime YUNUSA* *
https://ijojournals.com/ Volume 09 || Issue 03 || March, 2026 ||
"CYBER CRIME AND SECURITY AMONG NIGERIAN BANKING SYSTEM"

Ama, G. A. N., Onwubiko, C. O., & Nwankwo, H. A. (2024). Cybersecurity challenge in Nigeria deposit money banks. *Journal of Information Security,* 15, 494–523.

Aneke, C. A., Eze, J. O., & Nwoye, A. N. (2025). Socioeconomic determinants of cybercrime in Nigeria. FUOYE Journal of Criminology and Security Studies, 3(1), 1–15.

Central Bank of Nigeria. (2024). Exposure draft of the risk-based cybersecurity framework and guidelines for deposit money banks and payment service banks. https://www.cbn.gov.ng/Out/2024/BSD/EXPOSURE%20DRAFT%20OF%20THE%20RISKBASED%20CYBERSECURITY%20FRAMEWORK%20AND%20GUIDELINES%20FOR%20DEPOSIT%20MONEY%20BANKS%20AND%20PAYMENT%20SERVICE%20BANKS.pdf

Sunday, D., Offia, A. C., & Ekwunife, E. N. (2025). Cybersecurity threats and fraud detection: A study of selected banks in Nigeria. (2025). *Journal of Accounting and Financial Management*, 11(11), 269–290.

Darktrace. (2025). Cybersecurity for financial services: Definitions & examples. https://www.darktrace.com/cyber-ai-glossary/cybersecurity-for-financial-services

Economic and Financial Crimes Commission. (2024). About the EFCC. https://www.efcc.gov.ng

Encyclopaedia Britannica. (2025). Cybercrime. https://www.britannica.com/topic/cybercrime

European Parliamentary Research Service. (2024). Understanding cybercrime (Briefing PE 760.356). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

Federal Deposit Insurance Corporation. (2025). Information technology (IT) and cybersecurity. https://www.fdic.gov/banker-resource-center/information-technology-it-and-cybersecurity

Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Laws of the Federation of Nigeria. https://www.financierworldwide.com/the-nigerian-cybercrime-act-2015-and-its-implications-for-financial-institutions-and-service-providers

Garba, A. M., Sadiq, A. A., & Bello, R. S. (2023). Awareness of cybercrime among online banking users in Nigeria. *Nigerian Journal of Technology,* 42(4), 1031–1040.

Jaiyeola, T. (2024). Nigerian banks face 182% more weekly attacks than global counterparts. BusinessDay. https://businessday.ng/news/article/nigerian-banks-face-182-more-weekly-attacks-than-global-counterparts/

Owolabi, I. A. (2024). Essential tips for preventing online banking fraud in Nigeria. https://midmaconsulting.com/nigeria-online-banking-fraud-prevention-tips/

Mustapha, A., & Sinha, S. (2024). Cybercrime and digital banking security challenges in Nigeria. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4929630

Ngwu, F. N., Okorie, N. E., & Ojukwu, C. O. (2025). Bank verification number scams and financial system stability in Nigeria. International Journal of Multidisciplinary Research and Growth Evaluation, 6(2), 112–121. https://www.multiresearchjournal.com/admin/uploads/archives/archive-1751635243.pdf

Njidofor, O. C., Iyke-Ofoedu, M. I., & Uzochukwu, A. C. (2025). Cybercrimes and sustainable development of deposit money banks in Nigeria. Direct Research Journal of Management and Social Sciences, 12(2), 45–61. https://www.dzarc.com/education/article/view/658

Okafor, C., & Ugbaja, S. (2025). Cyber crime and digital banking fraud in Nigeria. Journal of Economics, Management and Trade, 31(3), 21–35.

Okpa, M. M.-O. (2024). An assessment of cyber crime in commercial banks in Calabar metropolis. *Ibom Journal of Social Issues,* 11(4), 20–25.

Ogunmokun, O. (2024). Cyber-enabled financial crimes and their effects on digital banking adoption in Nigeria. Elite Project. https://eliteproject.com.ng/cyber-enabled-financial-crimes-and-their-effects-on-digital-banking-adoption/

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies. *World Journal of Advanced Research and Reviews,* 21(2), 1225–1236.

Sambo, Z. (2025, October 2). Bank customers lose ₦250 bi annually to cyber crime. Economic Confidential. https://economicconfidential.com/bank-customers-cybercrime/

SilverTerrier. (2025). In Wikipedia. https://en.wikipedia.org/wiki/SilverTerrier

Statista Research Department. (2025). Digital banking fraud and cybersecurity trends in Nigeria. In Digital 2024 global overview report. https://link.springer.com/article/10.1007/s44282-025-00195-4

United Nations Office on Drugs and Crime. (2024). Cybercrime and anti-money-laundering strategies. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

Waliullah, M., Hossain George, M. Z., Hasan, M. T., & Islam, M. S. (2025). Assessing the influence of cyber security threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions,* 1(1), 226-257.