IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Evolving Threats in Mobile Banking: Examining WhatsApp Phishing Techniques and Countermeasures in Nigeria's Financial Sector

[1]Palang N. Mangut, [2]Sophie S. Nandom, [3]Emmanuel Mathias
[1]Plateau State University, Bokkos, Nigeria

Abstract: WhatsApp, which is widely used in Nigeria, is a prime phishing target in the banking sector. This study examines cybercriminal strategies in WhatsApp phishing targeting Nigerian banks, focusing on social engineering tactics and malware delivery. Using a qualitative approach, two case studies were analyzed: a social media scam impersonating GTBank and a syndicate attack uncovered by the Nigeria Police Force's National Cybercrime Center. The findings revealed how attackers invest in a complex social engineering attack framework that takes advantage of human psychology, institutions poor cybersecurity habits and of WhatsApp trust-based design. Evident social engineering ploy used by the attackers include urgency, impersonation, emotional manipulation as well as being confident of WhatsApp End-To-End Encryption to hide their footprints. The inquiry revealed intricate, layered schemes that took advantage of human psychology, institutional vulnerabilities, and the trust-based framework of WhatsApp. Delivery vectors for malware are identified as malicious links, dangerous Android packages, smishing and compromised documents all purposed at harvesting victim's credentials. This study contributes to understanding regional cybercrime variations and offers insights for developing countermeasures against WhatsApp phishing in emerging economies with similar technological and social characteristics.

IndexTerms **- WhatsApp, Phishing Attacks, Nigerian Banks, Technical Mechanisms, Social Engineering, Malware Delivery, Cybercriminals, Mitigation Strategies, User Awareness, Security Measures, Regulatory Frameworks.**

I. INTRODUCTION

INTRODUCTION

Nigerian banking has evolved from manual to digital systems, largely because of the 2006 banking consolidation (Ojabello, 2025). The industry leverages mobile technologies and social messaging platforms, such as WhatsApp, for business delivery. However, this has created opportunities for cybercriminals (Okpa, 2022). Phishing uses social engineering to obtain confidential information for theft or fraud (APWG, 2025). It has become pervasive, exploiting human vulnerability through social engineering (Njuguna et al., 2022). In Q1of 2025 phishing attacks rose to 1,003,924 incidents (APWG, 2025). Criminal actors adapt this method to bypass security measures (CheckPoint, 2025). The human element ensures the persistence of phishing, creating a cycle of criminal intelligence with minimal technological advantage. Nigeria's cashless society target missed its 95% financial inclusion goal for 2024 (Obiora & Ozili, 2024). Banks have introduced WhatsApp banking services (Okeke, 2025; Udenze et al., 2020), with 95.3% of Nigerian Internet users on the platform (Clement, 2020). Nigerian banks have integrated AI technology with WhatsApp, implementing chatbots such as Leo (UBA), Habari (GTB), and Ada (First Bank) to facilitate customer interaction and provide efficient services (Okeke, 2025).

This study aimed at investigating the technical mechanisms of WhatsApp phishing attacks against Nigerian banks. Analyses focusing on social engineering tactics and malware delivery approaches used in these attacks. This study explored two questions: What social engineering methods are used in WhatsApp phishing attacks on Nigerian bank and customers? How do cybercriminals use WhatsApp to deliver malware? A study of related literature and technical documents showed consistent social engineering tactics employed by cyber actors, malware operations, and credential harvesting techniques. A case study of two incidents provided context for banks, users and regulatory institutions. The study identified what vulnerabilities attackers leverage on in countries such as Nigeria. Consequently, it reveal's strategies that can mitigate such attacks. It emphasizes advanced social engineering attacks within Nigeria's business sector and pinpoints significant technical threats, such as information-stealing malware. This case study contributes to the understanding of regional variations in cybercrime and provides insights for developing effective countermeasures against WhatsApp phishing attacks in emerging economies with similar technological and social characteristics.

BACKGROUND ON PHISHING AND WHATSAPP SECURITY

2.1. WhatsApp Phishing Attacks

The digital transformation of Nigeria's financial sector has introduced cybersecurity risks, particularly through WhatsApp (Mustapha & Sinha, 2024). Phishing attacks commonly target WhatsApp users (Hussain et al., 2024; Outay & Malik, 2025). This

study focused on smishing and vishing attacks through WhatsApp. Vishing uses voice for scams, whereas smishing sends deceptive messages to obtain personal information or spread malware (Alabdan, 2020; Njuguna et al., 2022).

In Nigeria, cybercrimes and scams are perpetuated by criminal groups, such as Yahoo Yahoo, that often employ social engineering (Zhou et al., 2024). WhatsApp phishing scams vary by geographical location and include impersonation scams, WhatsApp Gold, phishing links, fake promotions, hoaxes, job offers, crypto scams, dating scams, verification code scams, and gift card scams (Outay & Malik, 2025). Common examples in Nigeria include impersonation scams, where scammers pose as family members or friends requesting urgent money transfers, often after hijacking WhatsApp accounts, as shown in Figure 1. Fake jobs, promotions, and government initiatives are prevalent as scammers exploit citizens' desire to escape hardship, as shown in Figure 2.

Figure. 1- Impersonation scam example, Source: (Jonathan, 2023)

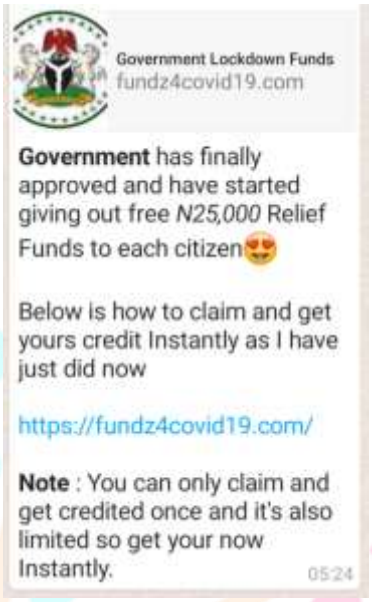

Figure 2 - Fake promotion phishing message example (with phishing link), Source: WhatsApp Group Platform

The primary objectives of phishing scams are: 1) to acquire personal information for identity theft or sale on the dark web, and 2) to install malware on victims' devices. The malware has capabilities to harvest personal data (infostealer), launch a denial-of-service (DoS) attacks, money extortion or run ransomware script that encrypts victim's device and get decrypted only when they pay. The underlying motive is financial gain (Alawida et al., 2022; Bhardwaj et al., 2020; Mangut & Datukun, 2021).

2.2 Nigerian Banking Sector

Nigeria has been a major cybercrime hub for decades, as previously documented. Cybercrime is said to costs the Nigerian economy about USD 500 million annually (Wang et al., 2020). The Nigerian Inter-Bank Settlement System Plc. (NIBSS), established in 1993 for inter-bank fund transfers, reported that while fraud incidents decreased between 2021 and 2023, financial losses increased. Losses grew from N2.96 billion in 2019 to N17.67 billion in 2023, with the loss ratio rising from 0.0019% to 0.0022% (NIBSS, 2023). The NIBSS remains the only government-affiliated agency with public data on bank cybercrime losses. Business Day Nigeria reported bank losses of N193.5 billion in 2021, N273 billion in 2022, and a projected N300 billion in 2023. In 2024, Nigerian banks lost N53.4 billion to cybercriminals within nine months (Admin, 2024). This apparent data discrepancy reflects that only 60 of the 163 profiled institutions reported fraud incidents to the NIBSS in 2023. Such data are crucial, as Nigeria lacks comprehensive fraud databases, such as the UK's National Fraud Intelligence Bureau (NFIB) Fraud and Cybercrime Dashboard (NFIB Dashboard, 2025).

3 Technical Mechanism

WhatsApp, founded in 2009 and acquired by Meta Platforms Inc. in 2014 (Britannica, 2025), was quickly adopted for banking in India, with Nigerian banks following suit in 2018 (Clickatell, 2018). WhatsApp's desired features promoting businesses, large user base and privacy protection. All these makes it appealing to businesses. Banks have transitioned from rule-based chatbots to large language models and Generative AI (Hasal et al., 2021), integrating them through WhatsApp Business and Cloud APIs(Hari & Abdulla, 2023). Spear phishing a targeted type of phishing was the main malware distribution method, used by 71% of groups in 2018 and 65% in 2019 (Alabdan, 2020). Banks encounter more cyber-dependent attacks than cyber-enabled attacks (Wang et al., 2020). In 2024, Nigeria reported an increase in cyberattacks (Osho et al., 2023; Ozibo, 2024), with WhatsApp's mobile platform offering opportunities for phishing exploitation.

3.1 Social Engineering Tactics

Social engineering is pivotal in WhatsApp phishing attacks on Nigerian bank customers' accounts. The human weakness makes it convenient for cybercriminals to bypass advanced security measures (Alkhalil et al., 2021). Strategies include impersonation, urgency, and emotional manipulation, which are adapted to Nigeria (Hussain et al., 2024). The following are the prevalent tactics:

3.1.1 Impersonation of Authority and Trust

Perpetrators impersonate individuals whom the victim's trust. Attackers use bank logos as WhatsApp profile images and professional language, posing as "Customer Care," "Fraud Department," or "Verification Team" representatives. They add users to

fake WhatsApp groups that mimic bank support with bank branding (Adu-Manu et al., 2023). Victims are added to these groups, sourced from compromised groups or databases (Hussain et al., 2024). These groups send urgent messages requesting Bank Verification Numbers and card details. Criminals hijack WhatsApp accounts to solicit money from their contacts. Attackers create fake bank WhatsApp Business accounts with branded logos, and users struggle to identify these fakes due to limited cybersecurity awareness (Olofinlade et al., 2025)or even technical experts (Alabdan, 2020). They are often trusted solely because they are business accounts (Outay & Malik, 2025). Criminals also impersonate Central Bank of Nigeria (CBN) or Nigeria Deposit Insurance Corporation (NDIC) officials, citing false policies requiring immediate action (CBN, n.d.). Both the CBN and NCC have warned against such schemes.

3.1.2 Creating Urgency and Scarcity

This tactic effectively leverages human interaction and psychological manipulation rather than exploiting software vulnerabilities. Inducing panic is a social engineering technique that hackers use to disrupt critical thinking (Hussain et al., 2024). The "Account Deactivation or Suspension" ploy sends messages claiming a user's bank account faces security breach risks or deactivation due to CBN directives, with deadlines to incite panic among users. This leads to account takeovers and data thefts. Research by Javelin Strategy revealed that financial losses reached $5.1 billion in 2017(Wang et al., 2020). Attackers send fake transaction alerts with "cancellation links" to phishing websites. Customers often fall victim to fraud (Mustapha & Sinha, 2024). Scammers create fake bank promotions with time-limited offers to rush users into clicking (Tuleun, 2022). Through tagging and trust engineering, attackers send messages appearing from trusted sources (Njuguna et al., 2022, 2022) to targets (Alawida et al., 2022).

3.1.3 Exploiting Greed and Opportunity

Appealing to financial gain is a classic social-engineering tactic. Attackers know the psychology of greed, vulnerable users will click on links with enticing promises, rewards or discounts too good to be true. The lure is clicking malicious links or downloading harmful files (Mustapha & Sinha, 2024). The victim's desire for gain compels them to follow the phisher's instructions. Criminals circulate deceptive offers about fictitious government grants, empowerment schemes, or relief funds, luring victims to click links that harvest their banking details (Alabdan, 2020; Alkhalil et al., 2021). Scammers also post fake job vacancies and then contact applicants via WhatsApp to collect sensitive personal and financial data. The victim's desire for gain leads to the attack success(Alabdan, 2020; Khan et al., 2020).

3.1.4 Pretexting and Information Gathering

Attackers engage in conversations to establish rapport and extract information before launching attacks, using fabricated scenarios to manipulate victims. An attacker might claim that the victim has won money and demand personal information (Alabdan, 2020). In the "Wrong Number" tactic, attackers pretend to misdial, build trust, and later send malicious links or request financial details for smishing attacks (Hussain et al., 2024). Messaging app phishing has increased, leading to identity theft (Outay & Malik, 2025). In fake Know Your Customer (KYC) updates, criminals pose as bank representatives (Osho et al., 2023) and request personal details via chat or phishing links(Wang et al., 2020). These tactics evolve as cybercriminals adapt to current events in Nigeria's digital landscape.

3.2 Malware Delivery Methods

Malware, malicious software that encrypts files, steals data, or gains unauthorized access, poses a cyber threat to organizations and banks (Alawida et al., 2022; Qammar et al., 2023). WhatsApp malware attacks compromise devices through social engineering and malicious software (Outay & Malik, 2025). These operations infect smartphones to steal financial information and drain accounts of their funds. In 2013, the POSRAM Trojan attack targeted bank payment cards, stealing data from 70 million customers (Eze, 2021). The Andromeda malware, renamed Gamarue/Wauchos in 2024, functions as a botnet with keyloggers, rootkits, and remote access capabilities(*ngCERT*, 2024). Globally, malware targeting PII has been reported, including 500 infected PyPI packages via typosquatting (CheckPoint, 2025). In Nigeria, the Anatsa banking Trojan attacked 70,000 devices, bypassing security as a PDF reader to steal financial information (Ozibo, 2024).

3.2.2 WhatsApp Malware Attack Framework

Attack framework of WhatsApp phishing is depended on deceptive files, exploitation of trust and other social engineering tactics. key stages recently employed by cybercriminals are as follows:

1. Initial Contact: The Social Engineering lure employs techniques from Section 3.1 to initiate its strategy. These methods evolve as society, needs, and circumstances change. Cybercriminals contact victims through carefully crafted messages that appear to be legitimate and urgent.

2. Malware Delivery Mechanisms: Attackers distribute malicious codes ‘malware’ through messaging platforms or as a link or embedded into a document or files. Smishing involves sending text messages containing malware or links to malware-hosting websites(Alabdan, 2020; Mangut & Datukun, 2021). Another method uses deceptive links directing users to attacker-controlled websites that initiate malware downloads(Alabdan, 2020; Tuleun, 2022). Malicious Android Packages disguise themselves as legitimate applications using identical identifiers (Al-Qahtani & Cresci, 2022). These malware can steal data, record audio and calls, take photos, and access messages (DelCotto, 2025; Dorobisz, 2024). Trojans can appear in advertising SDKs used in modified WhatsApp versions (CERRT.NG, 2021). PDF documents can serve as attack vectors through the embedding of malicious code. Cybercriminals embed malware in JavaScript code or links that initiate downloads. Outdated software can be exploited to execute code on victims' devices (CheckPoint, 2025). Attackers may also use forms with phishing rewards that install malicious software through vulnerabilities.

3. Types of Malware Deployed and Their Functions

Some malware used in these attacks are designed with capabilities for financial theft or targeted at banks or bank users, primarily to steal data.

- Keyloggers are a form of malware that records keystrokes on infected devices, capturing usernames, passwords, credentials, and PINs when users access banking apps. The stolen data are then exfiltrated for malicious purposes, such as unauthorized access (Alkhalil et al., 2021; Tuleun, 2022). These 'logs' are sold in underground marketplaces, leaving victims vulnerable to ongoing attacks. Keyloggers can also be integrated with other malware, such as Anubis, which has evolved from a banking Trojan to include keylogging and RAT capabilities, thereby benefiting cybercriminals (CheckPoint, 2025).

- Remote Access Trojans (RATs), classified under "Multipurpose Malware," are deployed early in attacks to download tools and extend control over compromised systems (CheckPoint, 2025). These RATs provide full control over infected devices, allowing the manipulation of files and processes and the execution of remote commands, including those for banking transactions (Tuleun, 2022). Once a system is infected, RATs establish backdoors that bypass firewalls to facilitate remote access (Alabdan, 2020). Noteworthy RATs include Rafel, Anubis, and AhMyth (CheckPoint, 2025).

- Stealers, or infostealers, extract sensitive data from compromised systems and operate within malware-as-a-service models (CheckPoint, 2025). They spread through phishing or malicious downloads, often offering enhanced features to attract users (Mustapha & Sinha, 2024; Seun & Dipo, 2024). The Snowflake breach exposed data from 165 organizations, and infostealer infections surged by 58% in 2024 (CheckPoint, 2025). Necro, a dropper malware, downloads additional payloads and has been found in unofficial repositories. Styx Stealer, derived from Phemedrone Stealer, retrieves passwords, cookies, and session data from messaging platforms such as Telegram and Discord (CheckPoint, 2025), indicating potential risks for WhatsApp.

- Overlay malware refers to malicious apps that exploit Android's overlay feature, which allows applications to draw an extra 'View' layer over others (Gong et al., 2022). This function is abused by malicious applications to compromise user security and privacy (Gong et al., 2022; Zhou et al., 2024). When the malware detects a legitimate banking app, it displays a fake login window over the real app, tricking the user into entering their credentials. The Joker malware is a notable example that subscribes users to premium services by simulating clicks and capturing SMS messages. This malware can be found in legitimate-looking applications on the Google Play Store, such as a 'Beauty Camera' app that received over 100,000 downloads (CheckPoint, 2025).

3.3 Why WhatsApp is an Effective Delivery System

Cybercriminals favor WhatsApp for several reasons, such as:

- Massive User Base: WhatsApp's widespread use makes it a prime target for hackers. Approximately 84% of respondents consider WhatsApp essential for daily communication (Hussain et al., 2024). Its ease of access increases security risks (Outay & Malik, 2025). In Nigeria, 95.3% of monthly internet users were registered on the platform as of 2024 (Ceci, 2025). It is preferred by small businesses (Udenze et al., 2020)and is widely used by university students. Nigerian banks now offer services through WhatsApp chatbots, such as Tamara, Ivy, Leo, and ZIVA (Ben-Enukora et al., 2022).

- End-to-End Encryption (E2EE): Although WhatsApp provides E2EE to secure conversations, certain threats can bypass this security (Hasal et al., 2021; Qammar et al., 2023; Udenze et al., 2020). A compromised device can still affect WhatsApp because it cannot filter malicious content. Despite being secure, system failures can allow hackers to steal user credentials (Bokolo & Daramola, 2024).

- Trust Factor: Users are less suspicious of messages from contacts, which criminals exploit by hacking accounts to spread malware (Outay & Malik, 2025).

CASE STUDIES

This section examines two specific incidents reported by the National Cybercrime Center (NCCC) and the Foundation for Investigative Journalism (FIJ), providing insights into attack mechanisms, regulatory responses, and mitigation strategies within the Nigerian context. The choice of cases is dependent on the prevalence of these attack types and their impact on the general public's trust and reputation.

4.1 Case Study Methodology

Incident Selection Criteria

- Documented cases with official law enforcement or media reporting
- Incidents involving WhatsApp as the primary attack vector
- Cases targeting Nigerian banking customers
- Availability of technical details about attack mechanisms

Data Sources

- National Cybercrime Centre (NCCC) official press releases
- Foundation for Investigative Journalism (FIJ) investigative reports
- Academic literature on social engineering and phishing attacks
- Nigerian banking regulatory frameworks and guidelines

4.2 Prominent WhatsApp Phishing Attacks

Case Study 1: The Social Media Redirection Scam (Impersonating GTBank).

A GTBank customer's social media post about a failed point-of-sale transaction led to fraudsters targeting them. The customer was contacted by a GTBank impersonator who stole ₦30,000 through WhatsApp-based social engineering.

- **Source:** Foundation for Investigative Journalism (FIJ) report (Abatta, 2025).
- **Case Type:** Multi-Platform Customer Support Impersonation and Financial Fraud.
- **Primary Attack Vector:** Social Engineering via Public Social Media (X/Twitter) and Encrypted Messaging (WhatsApp).

Incident Overview: Fraudsters using a fake GTBank support account on X responded to a customer's tweet, directing them to contact a "support agent" via a provided number. On WhatsApp, the impersonator posed as a bank representative, showing a forged staff ID card with a name and ID number for credibility. The scammer convinced the victim to share codes sent to their phone, likely One-Time Passwords. Using these codes, the fraudster gained unauthorized access to the customer's mobile banking application, enabling illicit transactions and causing financial losses.

Technical Attack Mechanisms

Initial Contact Phase:

- Social Media Monitoring: Monitoring Twitter/X for banking complaints, probably with an automated scanning tool.
- Profile Analysis: The perpetrator gathered victim information from public social media profiles and lured the victim to the WhatsApp platform under the guise of solving the victim's complaint.
- Timing Exploitation: Contacted victim within hours of complaint posting

Impersonation Phase:

- Fake Credentials: Produced convincing GTBank staff identification documents
- Official Communication Mimicry: Used formal language and banking terminology
- WhatsApp Business Account: Employed business account features to appear legitimate

Authentication Bypass:

- PIN Harvesting: Convinced victim to share transaction PIN under the pretense of "verification"
- OTP Interception: Guided victim through process of sharing One-Time Passwords
- Delay Tactics: Maintained active communication to prevent victim from contacting actual bank

Social Engineering Techniques

Authority Impersonation:

- Presented as official bank representative with employee ID
- Used banking jargon and internal process references
- Demonstrated knowledge of victim's recent transaction history

Problem-Solution Framework

- Acknowledged victim's legitimate complaint to build rapport
- Positioned fraudster as helpful bank employee solving the problem
- Created urgency by suggesting account security risks

Psychological Pressure:

- False Trust: Made victim to feel he was resolving the unsuccessful transaction
- Helpful Demeanor: Maintained friendly, professional communication tone
- Process Legitimization: Made fraudulent requests seem like standard banking procedures

Technical Vulnerabilities Exploited

- Customer Service Gaps: Lack of immediate bank response to social media complaints
- Communication Channel Confusion: Unclear guidelines on legitimate bank communication methods

Case Study 2: The Nigeria Police Force, National Cybercrime Center (NPF-NCCC) Disruption of a Notable WhatsApp Account Hijacking Syndicate.

Source: NPF-NCCC Press Release, April 2025 (NPF-NCCC 2025).

Case Type: Coordinated Hijacking of WhatsApp Accounts and Associated Financial Fraud. **Primary Attack Vector**: Social Engineering Tactics and Compromise of Mobile Platforms.

Incident Overview

In April 2025, the Nigeria Police Force National Cybercrime Center (NPF-NCCC) skilfully identified, scrutinized, and dismantled a highly sophisticated cybercriminal syndicate that specialized in hijacking WhatsApp accounts belonging to prominent citizens of Nigeria. Following the unauthorized account takeover, the syndicate assumed the identities of legitimate account holders to perpetrate fraud against their contacts. This operation, which was instigated by an official grievance, culminated in the apprehension of the principal suspect, the seizure of millions of naira in illicit proceeds, and the revelation of a complex criminal organization that exploited both technological vulnerabilities and human trust to execute its nefarious activities.

Technical Attack Mechanisms

The operational methodology of the syndicate was characterized not as a singular incident but as a systematically defined, reproducible process. Advanced digital forensic analyses conducted by the NPF-NCCC elucidated a clear multistage attack framework.

Account Compromise Phase:

- SIM Swapping: Attackers obtained duplicate SIM cards by impersonating victims at telecommunications service providers
- Social Engineering: Used publicly available information to answer security questions and verify identity
- Credential Harvesting: Employed phishing websites mimicking WhatsApp Web to capture login credentials OR
- One-Time Password (OTP) Scam: The perpetrator attempts to register the victim's WhatsApp account on a new device, triggering an SMS containing a 6-digit verification code sent to the victim's phone. Subsequently, the fraudster contacts the victim (using an alternate number or a compromised account belonging to a mutual acquaintance.

Exploitation Phase:

- Identity Impersonation: Utilized compromised accounts to impersonate trusted contacts
- Message Spoofing: Crafted convincing messages mimicking the communication style of account owners
- Urgency Creation: Fabricated emergency scenarios requiring immediate financial assistance

Technical Infrastructure:

- Virtual Private Networks (VPNs): Masked geographical locations and IP addresses
- Cryptocurrency Wallets: Facilitated anonymous money transfers and laundering

Social Engineering Tactics

Trust Exploitation:

- Leveraged existing relationships between account owners and their contacts
- Used personal information gathered from social media profiles
- Mimicked communication patterns and language preferences

Psychological Manipulation:

- Authority Bias: Impersonated respected figures to increase compliance
- Scarcity Principle: Created time-limited opportunities to pressure victims
- Reciprocity Exploitation: Referenced past favors or relationships to encourage assistance

Financial Impact

- Millions of naira accounted across various bank accounts
- Cross-border financial transfers complicating fund recovery efforts

RESULTS AND DISCUSSION

5.1 Cross-Case Analysis and Discussion

A comparative examination of the "GTBank Social Media Redirection Scam" and "NPF-NCCC Syndicate Takedown" reveals Nigeria's financial security threat landscape. While both exploit WhatsApp, they differ in their operational complexity and targeting methods. These cases represent cybercriminal conduct, ranging from opportunistic fraud to organized crime. Both attacks rely on psychological manipulation and abuse of trust: GTBank used the bank's identity, while NPF exploited interpersonal trust between contacts. Both used WhatsApp for fraud execution and targeted financial theft through Nigerian banks. The GTBank case represents an opportunistic model targeting distressed individuals, whereas the NPF case shows organized crime with recruitment and strategic targeting. GTBank fraudsters impersonated bank personnel, while the NPF impersonated account holders. The GTBank approach requires individual engagement, whereas the NPF framework scales through compromised accounts. Critical themes show that human vulnerability remains primary in cybersecurity, WhatsApp's trusted design enables fraud, and digital identity control is crucial, as compromised identities transform contact networks into targets. Table 1 provides an overview of the comparison, while Tables 2 and 3 highlight the technical mechanisms and social engineering findings, respectively.

Table 1: Case Overview Comparison

Aspect	Case 1: GTBank Impersonation	Case 2: NPF-NCCC Syndicate
Incident Type	Individual staff impersonation	Account hijacking syndicate
Primary Target	Individual banking customer	High-profile individuals
Attack Vector	WhatsApp + social media monitoring	WhatsApp account compromise
Financial Impact	₦30,000 (single victim)	Millions (multiple victims)
Attack Duration	Single incident (hours)	Extended operation (months)
Victims Count	1 individual customer	20+ high-profile individuals
Detection Method	Victim self-reporting	Official complaint to NCCC
Response Time	Immediate (victim reported)	72 hours average
Prosecution Status	Under investigation	Active investigation
Recovery Rate	No fund recovery	Partial fund recovery

Table 2: Technical Attack Mechanisms

Attack Phase	GTBank Impersonation Techniques	NCCC Syndicate Techniques
Reconnaissance	Automated social media complaint scanning	Social media profiling, contact analysis
Initial Access	Social media monitoring, victim identification	SIM swapping, credential harvesting
Persistence	Continuous WhatsApp communication	Account takeover, communication history analysis
Privilege Escalation	Authority figure impersonation	Trust relationship exploitation
Defense Evasion	Professional communication mimicry	VPN usage, identity masking
Credential Access	Banking PIN/OTP harvesting	WhatsApp login credentials
Collection	Transaction details, account information	Contact lists, personal information
Command & Control	Direct WhatsApp communication	Encrypted messaging platforms
Exfiltration	Banking credential theft	Financial information extraction
Impact	Direct account access and theft	Unauthorized fund transfers

Table 3: Social Engineering Tactics Analysis

Psychological Technique	Implementation Method	Success Factors	Countermeasures
Authority Impersonation	Fake bank staff credentials, official language	Cultural respect for authority	Staff verification protocols
Trust Exploitation	Using compromised trusted accounts	Existing relationships	Multi-channel verification
Urgency Creation	Emergency scenarios, time pressure	Fear of financial loss	Cooling-off periods
Problem-Solution Framework	Acknowledging legitimate complaints	Victim's actual banking issues	Official communication channels
Social Proof	Reference to banking procedures	Familiarity with processes	Customer education programs
Reciprocity	Offering help with banking problems	Gratitude for assistance	Skepticism training
Scarcity	Limited-time opportunities	Fear of missing out	Decision delay protocols
Commitment Consistency	Following "standard procedures"	Desire to complete processes	Verification requirements

5.2 Comparative Analysis with Global Phishing Patterns

5.2.1 Regional Characteristics

Nigerian-Specific Factors:

In developed countries, mobile messaging platforms are more heavily relied upon than email-based phishing (Mangut and Datukun, 2021). The extensive GSM network in the country has resulted in a significant use of phone calls for social engineering attacks. Cybercriminals closely monitor social media to identify victims and gather the necessary data. They exploit Nigerian social hierarchies and respect for authority figures.

Global Comparison:

From a global perspective, there has been a noticeable increase in the sophistication of attacks, particularly on social messaging platforms, akin to international cybercrime syndicates (Mustapha & Sinha, 2024). Similar profit-driven motives adapted to local economic conditions have also been observed (Bruce et al., 2024). This serves as evidence of the rapid adoption of new technologies and platforms for criminal purposes (Okpa 2022).

5.2.2 Evolution of Attack Vectors

In comparing traditional and modern approaches, we observe a transition from e-mail-based phishing to the use of instant messaging platforms (Alkhalil et al., 2021; Outay & Malik, 2025) along with the integration of social media intelligence gathering. Although social messaging platforms were originally designed to enhance communication and business operations, cybercriminals have repurposed them for malicious activities (Chaurasia, 2021; Okeke, 2025).

In platform-specific adaptations, WhatsApp's end-to-end encryption complicates law enforcement investigations (Wijnberg & Le-Khac, 2021). The features of WhatsApp business accounts appear to lend legitimacy to fraudulent communications, as the platform does not differentiate between legitimate and fraudulent users (Wijnberg and Le-Khac, 2021). Additionally, voice message capabilities facilitate more convincing impersonations.

5.3 Institutional Vulnerabilities and Response Analysis

5.3.1 Banking Sector Vulnerabilities

Customer education gaps show that mobile users install apps without sufficient awareness of WhatsApp-based fraud techniques (Udenze et al., 2020). In case two, the bank customer fell victim due to a limited understanding of legitimate bank communication channels. Insufficient training on social engineering recognition is shown.

Technical Infrastructure Limitations are evident in delayed fraud detection systems (Young, 2025). Limited real-time monitoring of social media for fraud indicators (Giordani, 2024b) could have provided an escape for GTB customers. Inadequate customer service response times for digital complaints.
Challenges in regulatory compliance encompass the implementation of cybersecurity frameworks (Familoni & Shoetan, 2024). Resource constraints hinder investments in security infrastructure (CheckPoint, 2025). There is a need to prioritize cybersecurity budgets alongside military arsenals. The rapidly evolving threat landscape often outpaces regulatory updates, with new tactics and attack vectors emerging, compelling regulatory institutions and banks to remain updated.

5.3.2 Law Enforcement Response Effectiveness - NCCC Capabilities
The NPF-NCC also deployed Digital Forensics for advanced investigative techniques for tracing fraudulent activities, which is an effective practice as it aids in investigating the most complex cases (Tuleun, 2022). They have the ability to freeze illicit funds across multiple financial institutions to limit further financial losses. A limitation is their response in tracking cross-platform attacks in reference to the NPF-NCCC case.

5.4 Victim Psychology and Decision-Making Analysis
The victim's vulnerability to the psychological factors of cultural influences and economic pressure that were leveraged include (Alabdan, 2020; Osho et al., 2023):

- Respect for authority figures increasing susceptibility to impersonation
- Trust-based social relationships exploited by fraudsters
- Limited cybersecurity awareness in older demographics has revealed a large number of victims of NPF-NCCC cases.
- Financial stress makes individuals more susceptible to fraudulent opportunities, as in the case of the GTB customer who lost N30,000.00 and reported a case of N4, 000. 00.

5.4.2 Decision-Making Processes that pertain to cognitive biases were exploited: Victims were inclined to Authority Bias, leading to a tendency to comply with perceived authority figures (Alabdan, 2020; Lappeman et al., 2023).
Emotional Manipulation that resulted to fear of financial loss, gratitude for apparent help with banking problems and urgency created through time-sensitive scenarios observed on victims interaction (Alabdan, 2020; Lappeman et al., 2023)

5.5 Regulatory Frameworks
The regulatory framework is an important guideline that aids in governing cybersecurity in the Nigerian banking sector. It ensures the security and integrity of financial systems and customer data. This framework typically includes various policies and regulations that streamline cybersecurity practices in Nigerian banks (Reis et al., 2024). The CBN is the main regulator that sets guidelines for financial institutions to protect their customers (Mukoro, 2024; Writer, 2025). National Information Technology Development Agency (NITDA) complement information technology practices. Other Law enforcement supporting bodies include the Economic and Financial Crimes Commission (EFCC) and NPF-NCCC.
Risk-Based Approach Requirements
The regulatory framework of Nigerian banks integrates several critical aspects.

- **Information Governance (IG)**: This an important aspect, where it becomes effective This is a vital component, with effective IG being build based on formalized structures, accountability, privacy, ethics, transparency, monitoring, compliance, and suitability. Banks must address changes in their business infrastructure using the appropriate IG policies and standards to mitigate data breaches and improve profitability (Reis et al., 2024).
- **Compliance with Regulations**: Adhering to rules is significant and relates to business sustainability and improved financial performance of Nigerian banks. Part of the challenges in compliance is seen in how businesses fail to report cyber incidents, thereby limiting exposure that can provide the required improved regulatory momentum in the financial sector.
- **Cybersecurity culture**: Researchers advocate for more research on cybersecurity culture in Nigeria. Improving the need for cybersecurity education and awareness will empower citizens to combat cyber threats (Reis et al., 2024).
- **Know-Your-Environment**: Comprehensive asset identification and risk assessment
- **Preventive Controls**: Multi-layered security measures including firewalls and intrusion detection
- **Monitoring and Detection**: Real-time threat monitoring capabilities
- **Policy Responses to Banking Crises**: Includes 24-hour incident reporting requirements for the CBN. The framework also incorporates the policy responses to banking crises. Banks must structure incident response and business continuity plans that guide the restoration of services after an attack or system failure (Mukoro, 2024).
- **Data Protection and Privacy**: To ensure the protection and privacy of financial data, put in place Data Loss Prevention (DLP) solutions should be implemented. DLP tools aid in monitoring data movement in an organization to mitigate unauthorized transfers. Similarly, banks must ensure compliance with Data Privacy Laws, particularly Nigeria's Data Protection Regulations (NDPR) and international privacy standards, such as the General Data Protection Regulation (GDPR).

5.6 Legal Framework
Nigeria's cybersecurity landscape is governed by several key regulations (CBN, 2023; Group, 2024; Mukoro, 2024).

1. **Central Bank of Nigeria (CBN) Cybersecurity Framework**: Mandates minimum cybersecurity standards for financial institutions
2. **Nigerian Cybercrimes Act 2015**: Provides legal framework for prosecuting cybercriminals
3. **Nigeria Data Protection Regulation (NDPR)**: Governs data privacy and protection

The Nigerian Cybercrimes Act 2015 provides the legal basis for prosecuting WhatsApp phishing attacks, establishes penalties for identity theft and financial fraud, and enables international cooperation in cybercrime investigations.

Enforcement Gaps in executing legal laws are linked to limited resources for comprehensive investigation and prosecution of cybercrimes. Challenges in evidence collection from encrypted platforms and jurisdictional complexities in cross-border cases.
Regulatory Enhancements in the area of mandatory cybersecurity training for banking staff and customers. Regular penetration testing and vulnerability assessments are essential. Other measures include standardized incident response procedures across financial institutions and enhanced international cooperation frameworks whenever necessary.

5.7 Mitigation Strategies

With phishing attacks over social messaging platforms such as WhatsApp, an effective mitigation strategy for cybersecurity risks will involve a multi-faceted approach, pulling together user-centric strategies alongside technical protection. What will stand out will include user awareness and education, prevention, and technical security measures (Giordani, 2024a).

5.7.1 User Awareness and Education

User education plays a crucial role in preventing malware infections (CheckPoint, 2025). It is crucial for mitigating security threats, especially sophisticated attacks such as phishing (Alkhalil et al., 2021). By increasing security awareness among employees and customers, organizations can potentially mitigate the risks associated with malware attacks (Alawida et al., 2022).

- **Improving User Awareness**: Educational solutions aim to teach users how to recognize the features of malicious messages through training, workshops, and awareness activities (Njuguna et al., 2022). In July 2025, the Virtual Institute of Capacity Building in Higher Education (VICHBE) enrolled close to 5000 Nigerians and other six African countries higher education instructors into its Module 10 course titled: Basic Cybersecurity for Higher Education. The training provided a platform for a cross-section of the academic sector (lecturers and staff) to be deeply grounded in cybersecurity awareness and empowered for defenses. It was an applaudable initiative of the team that received further recommendations for such training to be included in Nigeria's higher educational curriculum as general studies (GST) (Imam, 2025). This is an example of Nigeria's steps to create more awareness and empower Nigerians to deal with cyberattacks. In a recent National Cybersecurity Conference in July 2025, the EFCC Director General called for a collaborative effort to fight cybercrimes, noting that cybersecurity is not just a technical issue but a governance issue as well (Tunji, 2025). Individual awareness of cyber threats has been identified as a major area that researchers and government institutions can focus on to coach the general public on cyber threats and preventive measures (Alawida et al., 2022; Tuleun, 2022).
- **Reducing susceptibility**: Educating end users alongside technical solutions will reduce susceptibility to attacks (Alkhalil et al., 2021). Continuous training and awareness are important to further enlighten human vulnerabilities and emerging dangers (Njuguna et al., 2022).
- **Effectiveness and Challenges**: Institutions can choose to consider the cost of training, which is costly, as noted by Alkhalil et al. (2021), but in the same vein, the cost of the effect of cyberattacks is financially and non-financially costly. Victims can experience social disruption, loss of confidence in technology, anxiety, worry, depression, and many other psychological traumas (Ashawa & Morris, 2021). Although it is easier to measure financial losses, the emotional aspect is rarely quantified to present a holistic view of the losses incurred due to these crimes.
- **Innovative Approaches**: Exploring training using game-based technology has been reported to be effective in creating cybersecurity awareness (Alani & Al-Azzawia, 2025). A collaborative approach to cyber awareness and campaigns for the public by the government and key stakeholders, such as banks, can increase knowledge and motivation. (Dipo & Onyedikachi, 2024).

5.7.2 Prevention and User Education

Prevention is inherently linked to user education, as an informed user is less likely to fall victim to attacks. Education gives users an edge in identifying cyber threats, thereby serving as a preventive measure (Njuguna et al., 2022). Human error mitigation: Humans, as the weakest link, have been attributed to many successful attacks owing to human errors. User training could serve a great role as a preventive measure to cyberattacks, but at the same time, being aware of constantly staying updated as threat actors also keep up their game (Alkhalil et al., 2021).
The studied incidence can provide customer protection measures by educating bank customers on two-factor authentication in financial transactions. Banks set transaction limits and cooling-off periods for large transfers, which can derail threats, as narrated in the NPF-NCCC case.

5.7.3 Technical Security Measures

Effective mitigation requires the integration of technical defenses with user-centric approaches (Giordani, 2024a). Education complements technical solutions (Alkhalil et al., 2021). The prevalence of attacks on messaging applications requires technical checks, even though the majority of attacks begin with some form of social engineering, all of which may lead to credential compromise and financial loss (Outay & Malik, 2025).

Technical Approaches to Mitigation

Various technological strategies have been proposed to combat phishing, mostly 'smishing' (SMS phishing), which shares similarities with messaging app phishing (Njuguna et al., 2022). Advanced phishing detection models can analyze text patterns, look for deceptive phrases, and verify URLs in real time to safeguard against phishing attacks. One such development is 'MobiFish', a tool designed to offer protection over mobile apps and online pages (Njuguna et al., 2022). A recommended technical solution in respect to the case study can be platform-level security fortifying WhatsApp business verification, an improved reporting mechanism for fraudulent accounts, and integration with law enforcement investigation tools. Other technical solutions such as a detection algorithm or AI fraud solution can be explored to detect unusual banking activities to alert banks and necessary authorities. Financial institutions can provide secure communication channels for bank-customer interactions and sensitize their customers.

5.8 Critical Evaluation

5.8.1 Strengths of Current Approaches

The CBN's comprehensive cybersecurity guideline is an example of a proactive regulatory framework, which is a clear standard for financial institutions to follow (Mukoro, 2024). Second, a cohesive partnership between the CBN, NPF-NCCC, and other international partners enhances response capabilities. Likewise integrating technological tools and methods such as digital forensic and AI detection systems enhances and speeds up investigations (Emoekpere, 2025)

5.8.2 Limitations and Evidence Quality

Due to under-reporting, many incidents go unreported for fear of reputation concerns. This negatively impacts the quality of research findings. This study could not investigate another variant of incident (such as a malware-related attack) because a reported real-life case was not available at the time of this work. Nigeria tops the crime chart but suffers from limited empirical data to support research; there is insufficient quantitative research on Nigerian-specific phishing patterns. Consequently, resource constraints limiting funding for comprehensive cybersecurity research and implementation are another huge drawback to the country's efforts to curb cybercrime.

5.8.3 Methodological Improvements Towards Data Collection: A robust approach will benefit from the following improvements:

- Development of standardized incident reporting frameworks
- Creation of anonymous victim reporting systems
- Integration of banking sector fraud databases
- Collaboration with telecommunications providers for attack pattern analysis

5.8.4 Research Gaps

While there has been much research on the impact and prevalence of cyber threats to banking and financial institutions, investigations in the context of 'messaging platforms' or WhatsApp are still limited, particularly as they relate to economies like Nigeria with their unique sociocultural nature. Although the security measures surrounding such platforms as WhatsApp E2EE make it formidable to a large extent, cybercriminals are constantly circumventing security and taking advantage of human psychology. As such, there is an enormous need for empirical investigations into these subjects. More work is needed to investigate the prevailing WhatsApp-related phishing attacks in Nigeria and globally. Although WhatsApp is secure because of its E2EE, attackers take advantage of other vulnerabilities to infiltrate users. Here are areas of possible investigations; The economic drivers of cybercrime participation, likewise the sociocultural factors of Nigeria require investigations on how the cultural norms influence phishing susceptibility. Digital literacy is correlated with fraud victimization. In addition, there is limited research on WhatsApp and SMS-based attack vectors connected to mobile-specific vulnerabilities. This study did not attempt to conduct an economic impact assessment of the reported incidents. This is another area lacking research on comprehensive cost-benefit analyses of cybersecurity investments. Effectiveness evaluation of current countermeasures.

5.8.5 Implications and Examples

Practical Implications for Financial Institutions: Although generally discussed as mitigation strategies, some specific implications for banks are as follows:

1. Implement comprehensive awareness programs about WhatsApp and SMS-based phishing
2. Develop robust multi-channel verification systems for customer communications
3. Deploy AI-powered real-time monitoring systems for detecting suspicious transaction patterns

Policy Recommendations

1. Strengthen regulatory enforcement mechanisms for cybersecurity compliance
2. Increase collaboration between government agencies and financial institutions
3. Enhance cross-border information sharing for cybercrime investigation

Technological Solutions

1. Implement AI-based systems for real-time phishing detection (Amaechi & Okeke, 2024)
2. Explore distributed ledger solutions for secure transaction verification such as blockchain technology
3. Deploy advanced biometric systems for customer verification

Examples of Successful Interventions

The NPF-NCCC case demonstrates an effective law enforcement response through:

1. Successfully Freezing of millions of naira across multiple bank accounts
2. Arresting key perpetrators
3. Gathered comprehensive digital evidence for prosecution

Recommendations

For Financial Institutions

1. Implement Comprehensive Staff Training: Regular cybersecurity awareness programs focusing on social engineering tactics
2. Deploy Advanced Detection Systems: AI-powered monitoring for suspicious WhatsApp and SMS communications
3. Establish Customer Verification Protocols: Multi-factor authentication for all financial transactions
4. Create Incident Response Teams: Dedicated cybersecurity units for rapid threat response

For Regulatory Bodies

1. Strengthen Enforcement Mechanisms: Increase penalties for non-compliance with cybersecurity frameworks
2. Enhance Inter-Agency Coordination: Improve information sharing between NCCC, CBN, and other agencies
3. Develop Mobile-Specific Guidelines: Create targeted regulations for WhatsApp and SMS-based financial communications
4. Invest in Capacity Building: Increase funding for cybersecurity training and infrastructure

For Customers and General Public

1. Verify All Financial Communications: Always confirm requests through official bank channels
2. Enable Security Features: Activate two-factor authentication on all financial applications
3. Report Suspicious Activities: Immediately report potential phishing attempts to relevant authorities
4. Stay Informed: Regularly update knowledge about emerging phishing techniques

CONCLUSION

This study examined technical mechanisms underlying WhatsApp phishing attacks targeting Nigerian banks through analysis of two case studies: a GTBank impersonation scam and a syndicate operation identified by the Nigeria Police Force National Cybercrime Centre (NPF-NCCC). The investigation uncovered intricate operations that exploit human behavior, institutional vulnerabilities, and the secure messaging system of WhatsApp. Notable methods used by these attacks will be manipulation, creating urgency, and claiming to be who they are not. They use malicious links, smishing fake applications to spread and downloads malwares.

. The study revealed sophisticated operations that exploit human psychology, institutional vulnerabilities, and WhatsApp's encrypted messaging architecture. The attacks used diverse approach combining such as social engineering tactics—including impersonation, urgency psychological manipulation, and emotional exploitation—with different malware delivery mechanisms such as smishing, deceptive links, malicious Android packages, and weaponized documents. These operations are distinguished by their mobile-first orientation, cultural adaptation of social engineering techniques, with social media intelligence gathering, and strategic exploitation of regulatory gaps. The Central Bank of Nigeria faces challenges enforcing cybersecurity framework guidelines established due to resource limitations and rapidly evolving nature of threats. Effective countermeasures require a comprehensive approach addressing Nigeria's unique socio-technical banking environment through enhanced customer education, robust authentication mechanisms, and strengthened inter-agency coordination.

The findings emphasize the critical need for platform-specific security measures and targeted user awareness programs. This research contributes valuable insights for developing effective countermeasures against WhatsApp-based financial fraud in emerging economies with comparable technological and regulatory contexts.

REFERENCES

1. Abatta, A. (2025, July 11). Lagos Resident Reported Failed PoS Transaction on X. Then Fraudster With “Fake” GTBank Staff ID Stole Her N30,000. *Foundation For Investigative Journalism*. https://fij.ng/article/lagos-resident-reported-failed-pos-transaction-on-x-then-fraudster-with-fake-gtbank-staff-id-stole-her-n30000/
2. admin. (2024, November 27). *Nigerian Banks Lose N53.4 Billion to Cybercriminals in Nine Months -Report—FINTECH MAGAZINE AFRICA*. https://fintechmagazine.africa/2024/11/27/nigerian-banks-lose-n53-4-billion-to-cybercriminals-in-nine-months-report/
3. Adu-Manu, K., Ahiable, R., Appati, J., & Mensah, E. (2023). Phishing Attacks in Social Engineering: A Review. *Journal of Cyber Security*, *4*(4), 239–267. https://doi.org/10.32604/jcs.2023.041095
4. Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), Article 10. https://doi.org/10.3390/fi12100168
5. Alani, A. A., & Al-Azzawia, A. (2025). Phishing Attacks Detection and Prevention Techniques: An Overview. *Journal of Al-Qadisiyah for Computer Science and Mathematics*, *17*(1), 166–178. https://doi.org/10.29304/jqcsm.2025.17.11972
6. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
7. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.
8. Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *Iet Information Security*, *16*(5), 324–345. https://doi.org/10.1049/ise2.12073
9. Amaechi, C. E., & Okeke, O. (2024). Leveraging NLP and Deep Learning for Phishing Detection and Anti-Phishing Training in Nigeria: A Focus on Localized Tactics and Cultural Factors. *International Research Journal of Innovations in Engineering and Technology*, *08*(10), 01–06. https://doi.org/10.47001/IRJIET/2024.810001
10. APWG. (2025, July 2). *APWG | Phishing Activity Trends Reports*. Https://Apwg.Org/Trendsreports/. https://apwg.org/trendsreports/
11. Ashawa, M., & Morris, S. (2021). Analysis of Mobile Malware: A Systematic Review of Evolution and Infection Strategies. *Journal of Information Security and Cybercrimes Research*, *4*(2), 103–131. https://doi.org/10.26735/KRVI8434
12. Ben-Enukora, C., Adeyeye, B. K., Ejem, A. A., & Maduadichie, F. E. (2022). AWARENESS, ADOPTION AND PERCEPTION OF WHATSAPP CUSTOMER SERVICE CHATBOTS IN THE BANKING SECTOR: PERSPECTIVES FROM UNDERGRADUATE STUDENTS IN LAGOS, NIGERIA. *Nigerian Journal of Communication Review*, *1*(No. 2).
13. Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N., & Arthi, S. (2020). Why is phishing still successful? *Computer Fraud & Security*, *2020*(9), 15–19. https://doi.org/10.1016/S1361-3723(20)30098-1
14. Bokolo, Z., & Daramola, O. (2024). Elicitation of security threats and vulnerabilities in Insurance chatbots using STRIDE. *Scientific Reports*, *14*(1), 17920. https://doi.org/10.1038/s41598-024-68791-z
15. Britannica. (2025, August 6). *WhatsApp | History, Meta Acquisition, Criticism, & Facts | Britannica*. https://www.britannica.com/topic/WhatsApp
16. Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE*, *19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312

17. CBN. (n.d.). *FINFENDER Review.pdf*. Retrieved July 29, 2025, from https://www.cbn.gov.ng/Out/2021/CPD/FINFENDER%20Review.pdf
18. CBN. (2023, August). *EXPOSURE DRAFT OF THE RISK-BASED CYBERSECURITY FRAMEWORK AND GUIDELINES FOR DEPOSIT MONEY BANKS AND PAYMENT SERVICE BANKS.pdf*. https://www.cbn.gov.ng/Out/2024/BSD/EXPOSURE%20DRAFT%20OF%20THE%20RISK-BASED%20CYBERSECURITY%20FRAMEWORK%20AND%20GUIDELINES%20FOR%20DEPOSIT%20MONEY%20BANKS%20AND%20PAYMENT%20SERVICE%20BANKS.pdf
19. Ceci, L. (2025, May 8). *WhatsApp usage in selected countries 2024*. Statista. https://www.statista.com/statistics/291540/mobile-internet-user-whatsapp/
20. CERRT.NG. (2021, September). *Cerrt-News-Letter-3rd-Q-1.pdf*. CERRT.NG. https://cybersecurity.nitda.gov.ng/wp-content/uploads/2022/03/Cerrt-News-Letter-3rd-Q-1.pdf
21. Chaurasia, Dr. S. (2021). Looking up to Social Media for Personal Branding: A Study on Gen-Z Audience. In *Sustainable Development: Challenges, Opportunity, and the Way Forward*. Bharti Publications. http://library.atmiya.net:8080/dspace/bitstream/handle/atmiyauni/2113/210%29%2051943_Tushar%20Babubhai%20Ranpariya.pdf?sequence=1&isAllowed=y#page=73
22. CheckPoint. (2025). *Cyber Security Report 2025*. Check Point Software. https://www.checkpoint.com/security-report/
23. Clement, J. (2020, November 9). *Nigeria mobile internet users 2025*. Statista. https://www.statista.com/statistics/972896/nigeria-mobile-internet-users/
24. Clickatell. (2018, October 30). *First Bank of Nigeria and Clickatell Drive Financial Inclusion in Nigeria Using WhatsApp*. https://www.clickatell.com/press-center/first-bank-launches-whatsapp-chat-banking/
25. DelCotto, G. (2025, July 8). Godfather Malware Hijacks Banking Apps—Here's What to Know. *Republic Bank of Chicago*. https://republicbank.com/godfather-malware-hijacks-banking-apps-heres-what-to-know/
26. Dipo, T., & Onyedikachi, A. M. (2024). Developing a Biblical Solution Model for Mitigating Phishing Risks Among Internet Banking Users in Nigeria: The Initial Investigation. *International Journal of Latest Technology in Engineering, Management & Applied Science*, *XIII*(IV), 61–75. https://doi.org/10.51583/IJLTEMAS.2024.130408
27. Dorobisz, J. (2024). ANALYSIS OF TRENDS AND RISKS IN THE FIELD OF NETWORK SECURITY BASED ON STATISTICAL DATA. *GIS Odyssey Journal*, *4*(2), 147–163. https://doi.org/10.57599/gisoj.2024.4.2.147
28. Emoekpere, E. (2025, July 19). *7 essential cybersecurity tips for Nigerians—Businessday NG*. Https://Businessday.Ng/. https://businessday.ng/bd-weekender/article/7-essential-cybersecurity-tips-for-nigerians/
29. Eze, P. A. U. (2021). Challenges of Cybercrime on Online Banking in Nigeria a Review. *IDOSR JOURNAL OF ARTS AND MANAGEMENT 2021, 6(1): 63-69*, 7.
30. Familoni, B. T., & Shoetan, P. O. (2024). CYBERSECURITY IN THE FINANCIAL SECTOR: A COMPARATIVE ANALYSIS OF THE USA AND NIGERIA. *Computer Science & IT Research Journal*, *5*(4), 850–877. https://doi.org/10.51594/csitrj.v5i4.1046
31. Giordani, J. (2024a). Advancing Mitigation Strategies for AI-Driven Chatbots: Building Resilience Against Data Privacy Violations. A Follow-up Study. *European Journal of Applied Science, Engineering and Technology*, *2*(6), Article 6. https://doi.org/10.59324/ejaset.2024.2(6).15
32. Giordani, J. (2024b). Mitigating Chatbots AI Data Privacy Violations in the Banking Sector: A Qualitative Grounded Theory Study. *European Journal of Applied Science, Engineering and Technology*, *2*(4), Article 4. https://doi.org/10.59324/ejaset.2024.2(4).02
33. Gong, L., Li, Z., Wang, H., Lin, H., Ma, X., & Liu, Y. (2022). Overlay-Based Android Malware Detection at Market Scales: Systematically Adapting to the New Technological Landscape. *IEEE Transactions on Mobile Computing*, *21*(12), 4488–4501. https://doi.org/10.1109/TMC.2021.3079433
34. Group, G. L. (2024, June 11). *International Comparative Legal Guides* (United Kingdom) [Text]. International Comparative Legal Guides International Business Reports; Global Legal Group. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria
35. Hari, A., & Abdulla, M. S. (2023, June). *WhatsApp as a Superapp: Chatbots, Business API and the challenges ahead*. Www.Iimk.Ac.In. https://iimk.ac.in/uploads/publications/IIMKWPS583ITS202306.pdf
36. Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V., & Ogiela, L. (2021). Chatbots: Security, privacy, data protection, and social aspects. *Concurrency and Computation: Practice and Experience*, *33*(19), e6426. https://doi.org/10.1002/cpe.6426
37. Hussain, F., Rahman, R., Attarbashi, Z. S., Fadaq, W. H. N., & Mustafa, M. (2024). Understanding Human Behavior in Phishing Attacks Across Diverse User Groups: An Ethical Hacking Analysis. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, 1–7. https://doi.org/10.1109/KHI-HTC60760.2024.10482040
38. Imam, A. (2025, July 30). 16 Unilorites shine at VICBHE – University of Ilorin. *Campus News*. https://www.unilorin.edu.ng/16-unilorites-shine-at-vicbhe/
39. Jonathan, S. (2023, October 30). How WhatsApp scammers circumvent security features to swindle Nigerians—Dubawa. *Dubawa - Amplifying The Truth*. https://dubawa.org/how-whatsapp-scammers-circumvent-security-features-to-swindle-nigerians/
40. Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic*. https://doi.org/10.36227/techrxiv.12278792.v1
41. Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2023). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing*, *28*(2), 337–357. https://doi.org/10.1057/s41264-022-00154-z
42. Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & Isabalija, R. (n.d.). *[PDF] Seeing Beyond the Surface, Understanding and Tracking Fraudulent Cyber Activities | Semantic Scholar*. Retrieved May 22, 2024, from

https://www.semanticscholar.org/paper/Seeing-Beyond-the-Surface%2C-Understanding-and-Cyber-Longe-Mbarika/963b43c06e8c1c59289346829e8e1455245283e6

43. Mangut, P. N., & Datukun, K. A. (2021). The Current Phishing Techniques – Perspective of the Nigerian Environment. *World Journal of Innovative Research*, *10*(1). https://doi.org/10.31871/WJIR.10.1.9
44. Mukoro, G. (2024, September 6). *UIDC Limited ~ Cybersecurity in Finance Companies: Adhering to the CBN Framework and Guidelines in Nigeria*. UIDC Limited. https://uidcfinancecompany.com.ng/news/detail/cybersecurity-in-finance-companies-adhering-to-the-cbn-framework-and-guidelines-in-nigeria
45. Mustapha, A., & Sinha, A. (2024). Cyberfraud in the Nigerian Banking Sector: The Techniques and Preventive Measures. *International Journal of Innovative Science and Research Technology (IJISRT)*, 171–179. https://doi.org/10.38124/ijisrt/IJISRT24AUG395
46. *ngCERT: Anatsa, malware stealing banking data, hits 70,000 Android devices - Technology Times | Latest and Breaking Nigeria Tech News*. (2024, July 11). https://technologytimes.ng/ngcert-warns-of-anatsa-banking-malware/
47. NIBSS. (2023). *2023-Annual-Fraud-Landscape.pdf*. https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf
48. Njuguna, D. N., Kamau, J., & Kaburu, D. (2022). A Review of Smishing Attaks Mitigation Strategies. *International Journal of Computer and Information Technology(2279-0764)*, *11*(1). https://doi.org/10.24203/ijcit.v11i1.201
49. NPF-NCCC. (2025). *POLICE UNCOVERS, DISMANTLES WHATSAPP FRAUD SYNDICATE TARGETING HIGH-PROFILE NIGERIANS*. https://nccc.npf.gov.ng/news/press-release-police-uncovers-
50. Obiora, K. I., & Ozili, P. K. (2024). Comparative Analysis of Financial Inclusion in Nigeria, Sub-Saharan Africa, and the World. *Perspectives on Global Development and Technology*, *22*(3–4), 217–238. https://doi.org/10.1163/15691497-12341659
51. Ojabello, O. (2025, March 6). The death of traditional banking: How Nigerian banks evolved in 20 Years. *Businessday NG*. https://businessday.ng/columnist/article/the-death-of-cash-counters-how-digital-banking-took-over-nigeria/
52. Okeke, L. (2025). AI-Powered Chatbots and Customer Experience in Nigeria's Banking Sector: Opportunities and Challenges. *Nnadiebube Journal of Social Sciences*, *6*(1), Article 1.
53. Okpa, M. M.-O. (2022). *AN ASSESSMENT OF CYBER CRIME IN COMMERCIAL BANKS IN CALABAR METROPOLIS*. *11*(4).
54. Olofinlade, S. O., Abere, M. A., & Ogunjimi, O. L. A. (2025). Threats+of+Using+Portable+Devices-Oluwapelumi.pdf. *African Banking and Finance Review Journal (ABFRJ) International Open Access Journal*, *20*(5), 12.
55. Osho, O., Odumesi, J., Lateef, H., & Ayodele, J. (2023). *Cyber Security Experts Association of Nigeria (CSEAN)—National Cyber Threat Forecast 2024*.
56. Outay, F., & Malik, H. (2025, March 28). *WhatsPhish: WhatsApp AI Phishing Detector Chatbot*. 2025 ASEE North Central Section (NCS) Annual Conference. https://peer.asee.org/whatsphish-whatsapp-ai-phishing-detector-chatbot
57. Ozibo, R. (2024, July 12). ngCERT raises alarm over Android malware targeting personal banking security, over 70,000 devices infected. *Nairametrics*. https://nairametrics.com/2024/07/12/ngcert-raises-alarm-over-android-malware-targeting-personal-banking-security-over-70000-devices-infected/
58. Qammar, A., Wang, H., Ding, J., Naouri, A., Daneshmand, M., & Ning, H. (2023). *Chatbots to ChatGPT in a Cybersecurity Space: Evolution, Vulnerabilities, Attacks, Challenges, and Future Recommendations* (arXiv:2306.09255). arXiv. https://doi.org/10.48550/arXiv.2306.09255
59. Reis, O., Oliha, J. S., Osasona, F., & Obi, O. C. (2024). CYBERSECURITY DYNAMICS IN NIGERIAN BANKING: TRENDS AND STRATEGIES REVIEW. *Computer Science & IT Research Journal*, *5*(2), Article 2. https://doi.org/10.51594/csitrj.v5i2.761
60. Seun, E., & Dipo, T. (2024). Machine Learning Model to Mitigate Fake Bank Alert Phishing Fraud in Nigeria: The Initial Investigation. *Indian Journal of Computer Science and Engineering*, *15*(2), 152–161. https://doi.org/10.21817/indjcse/2024/v15i2/241502007
61. Tuleun, W. (2022). *Analysis of Cybercrimes, Major Cyber Security Attacks and the Overall Economic Impact on Nigeria* (SSRN Scholarly Paper 4886894). Social Science Research Network. https://papers.ssrn.com/abstract=4886894
62. Tunji, S. (2025, July 9). Nigeria to deport foreign cybercriminals after jail term. *Punch Newspapers*. https://punchng.com/nigeria-to-deport-foreign-cybercriminals-after-jail-term/
63. Udenze, S., Onwuliri, E. C., & Ugoala, B. (2020). AWARENESS AND USE OF WHATSAPP FOR BANKING AND FINANCIAL SERVICES: A STUDY OF SOCIAL MEDIA USERS IN NORTH-CENTRAL NIGERIA. *Nnamdi Azikiwe University Journal of Communication and Media Studies*, *1*(1), Article 1. https://doi.org/10.47851/naujocommed.v1i1.69
64. Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415
65. Wijnberg, D., & Le-Khac, N.-A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, *38*, 301132. https://doi.org/10.1016/j.fsidi.2021.301132
66. Writer, G. (2025, March 26). Assessing CBN's cybersecurity framework and guidelines. *TheCable*. https://www.thecable.ng/assessing-cbns-cybersecurity-framework-and-guidelines/
67. Young, D. (2025). Analysis of Emerging Cybersecurity Threats in Nigeria's Financial Sector: Trends, Impacts, and Mitigation Strategies. *International Journal of Research and Innovation in Social Science*, *IX*(VII), 1094–1103. https://doi.org/10.47772/IJRISS.2025.90700089
68. Zhou, H., Wu, S., Qian, C., Luo, X., Cai, H., & Zhang, C. (2024). Beyond the Surface: Uncovering the Unprotected Components of Android Against Overlay Attack. *Proceedings 2024 Network and Distributed System Security Symposium*. Network and Distributed System Security Symposium, San Diego, CA, USA.