ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

Cyberfraud in the Nigerian Banking Sector: The Techniques and Preventive Measures

Ahmad Mustapha[1]
MCS (AIML and Cybersecurity)
Faculty of Computer Science and IT.
Kalinga University, Raipur, India.

Dr. Anupa Sinha[2]
Assistant Professor
Faculty of Computer Science and IT.
Kalinga University, Raipur, India

Abstract::- The cyberfraud techniques emerged as a significant threat to the banking sector in Nigeria. Bank customers have been losing their hard-earned funds to these measures due to a lack of sufficient awareness of the cyberfraud tactics and preventive measures. There has been an increased rate of loss recorded annually in the banking sector due to fraud. The banking sector in Nigeria recorded a loss to a tune amount of ₦17.6bn in 2023 amount higher than the budget allocation for education in most states of the country. Social engineering remains the persistent and predominant technique fraudsters employ to defraud bank customers in Nigeria. Phishing, identity theft, login credential theft, ATM card swap, and skimming are other techniques cybercriminals employ. This research paper aims to examine and analyze the modus operandi of these techniques and explore the strategic preventive measures that can be implemented by customers to mitigate these risks, such as using advanced cybersecurity technologies, multi-factor authentication systems, employee training, as well as regulatory controls. The paper highlights the significance of a proactive and adaptive cybersecurity posture, continuous monitoring, and collaboration with regulatory bodies to enhance the resilience of the banking sector against cyber threats. The research focuses more on cyberfrauds targeting bank customers, and secondary data will be used for research purposes.

Keywords:- *Fraud, cyberfraud, Bank, Social Engineering, Phishing.*

I. INTRODUCTION

The banking industry is a crucial component of the broader financial system and a major source of funding for commercial activities. The trade of goods and services is facilitated in part by a banking system that operates efficiently. Additionally, it offers financial incentives for saving and effectively directs funding toward profitable ventures. Therefore, in any economy, the financial system encourages and supports the effective distribution of resources.

According to the report published by NIBSS (Nigeria Interbank Settlement System), as of December 2022 banking sector in Nigeria had more than 151 million customers (NIBSS, 2023) which is about 65% of the Country's population. This result grows annually as compared to previous years. The Central Bank of Nigeria (CBN) also published an updated list of Deposit Money Banks (DMBs) in Nigeria on 26 April 2024. In the recent list published by the Apex Bank, 43 deposit money banks are included, and these banks are classified according to their operational license International, national, and regional reflecting their operational competence and the services they are allowed to offer. DMBs are financial institutions authorized by CBN to accept public deposits and create credit. They are fundamental to the banking ecosystem, which affects everything, from individual savings to corporate investments (Nairametrics, 2024).

One of the major threats to Nigerian banks and their customers is the issue of fraud which has been a principal threat in the sector causing a huge setback and loss to the sector, economy, and the country's reputation. Although the incident of fraud is not a problem peculiar to Nigeria it has been a global concern. However, the high rate of fraud within the banking industry calls for urgent attention with the view to finding solutions (Alhaji & Simon, 2018). As the rate has escalated to the level of making many customers of the bank lose confidence in saving money with the banks.

- *Merriam-Webster Dictionary Defines Fraud as*

- "An intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right".
- "An act of deceiving or misrepresenting".

"Fraud" is any activity that relies on deception in order to achieve a gain. Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (Black's Law Dictionary).

Cyberfraud is a subset of fraud that is more targeted at bank customers. Which is refers to the crime committed using digital devices. In other words, a crime that utilizes technology particularly (but not exclusively) the internet and computers. Cybercriminals use various attack techniques to carry out cyberattacks and are constantly seeking new methods to achieve their goals, while avoiding detection and arrest. (Brush & Kobb, 2024) Some of the common techniques employed by cybercriminals to extort bank customers include social engineering, Phishing, identity theft, login credential theft, Business email compromise (BEC),

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

ATM card swap & skimming among others. Learning these techniques and their mode of operation will guide bank customers to safeguard their funds and uphold the integrity of the banking sector.

➢ *Research Questions*

This study contributes to the current research efforts that strive to establish effective techniques for combating cyberfrauds targeting bank customers in Nigeria by providing an answer to the following questions:

- What are the techniques employed by cybercriminals to defraud bank customers in Nigeria?
- What impact do these cyberfraud tactics have on the bank and customers?
- What measures can customers take to protect themselves against cyberfraud?

➢ *Research Objectives*

This study aims to identify the common tactics used in cyber fraud targeting bank customers in Nigeria, their impacts on the banking sector, and propose effective preventive measures.

II. LITERATURE REVIEW

The advent of technology and the Internet of a Thing (IoT) led to increased use of mobile banking that relies on Internet connectivity. This makes the bank customers more vulnerable to cyberattacks. The banking sector of Nigeria is a cornerstone of the country's economy, as it manages and distributes financial resources to other economic sectors and helps the economy develop and flourish. According to Ogbonna, Mobosi and Ugwuoke (2020), banks are one of the most important and dominant segments of Nigeria's economy, with significant impacts on economic growth and changes. (Olumayokun, et al., 2023) The banking sector in Nigeria consists of 43 DMBs (CBN, 2023) aside from the Deposit Money Banks, CBN also licensed Fintech (Financial Technology) companies such as (Opay, Kuda, Moniepoint, Flutterwave, etc) which are unbundling financial services that used to go through the banks by providing more proficient and efficient services. Those Fintechs operate digitally thereby exposed to cyberfraud.

Fraud which is literary defined as “The intentional deception or misrepresentation made by an individual or organization for the purpose of gaining an unfair or illegal advantage, typically involving financial or personal gain” (OpenAI, 2024) is the major setback in the Nigerian Banking sector causing a huge loss to the sector, economy, and the country's reputation. The fraud is said to be cyberfraud when it involves the use of a Computer, network, or other digital devices.

Cyberfraud in the banking sector is of two different majors, categorized by the motive of cybercriminals the first category is where the bank is the target of the attack, and later where the customer is the target, this research focuses on cyberfraud where the bank customers are the targets of the attack.

According to a report published by Oxford University on 10th April, 2024, Nigeria is one of the leading countries in the world regarding cyberfraud and it’s among the top five countries where bank payment transactions are unsecured. (Oxford, 2024) The report by NIBSS (Nigeria Interbank Settlement System), shows that there was a total number of 95,620 reported fraud in 2023 where 80,658 customers are the victims. And this causes the country a loss of ₦17.67bn. (NIBSS, 2023) Fraud in the banking system is a severe global issue, with total losses amounting to a staggering $485.6 billion in 2023 from a variety of devastating scams and bank fraud schemes worldwide. (Nasdaq & Verafin, 2023). The Annual Fraud Landscape, 2023 of NIBSS also analyzed the Fraud in the banking sector based on the States, the primary target, the most vulnerable device, and the most common technique employed by cybercriminals where,

- The highest percentage of defrauded individuals resides in Lagos (23%), followed by Rivers (6%), Abuja (5%), Ogun (5%) and Oyo (5%).
- Based on the report, individuals over the age of 40 years are the most targeted demographic by fraudsters in 2023.
- Mobile device is the most exploitable device for cybercriminals.
- Social Engineering, remains a persistent and predominant technique employed by fraudsters. (NIBSS, 2023)

Fraud is committed for the following reasons: perceived pressure, anticipated opportunity, and rationalization. These three elements or basic concepts were taken from the "Fraudulent Triangle Theory" founded by Donald R. Cressey (Kyrychenko, et al.,2021).

➢ *Cyberfraud Techniques*

Cyberfraud in the banking system takes various forms particularly as new scheme emerges regularly, so the attackers evolve with different techniques to defraud customers. (Wingard, 2024) Below are some of the methods employed by cybercriminals targeting customers in the banking sector.

- *Social Engineering:*

A social engineering attack is a method used by cybercriminals that doesn't rely on cracking passwords or exploiting software vulnerabilities, rather it focuses on manipulating human beings into divulging sensitive information or performing certain actions.

Christopher Hadnagy, in his book Social Engineering: the Science of Human Hacking defined social engineering as “any act that influences a person to take an action that may or may not be in his or her best interests”. (Hadnagy, 2018)

✓ *Baiting*

Baiting is a popular social engineering approach that capitalizes on someone's greed or interest. The attacker will entice the victim with something appealing or valuable (bait) and use this response to their advantage. (Fortra, 2024)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

One of the simplest yet most powerful types of bait assault is web-based adverts that promise large sums of money or other appealing things in exchange for the end-user installing a malware-infected program. Malicious applications often have added features compared to the original version to entice the victim into installing it on their devices. A typical example of such an application is '***GBWhatsapp***', which provides users with more enticing features than the real WhatsApp application. The victim's device will then be infected with malware, which can provide the attacker with personal information such as credit card numbers, login credentials, and other Personally Identifiable Information (PII).

✓ *Phone Call*

Social engineering via a telephone is also known as Phone scam or Vishing, it is a type of attack in which the attacker poses as a legitimate customer care representative of a particular bank and tricks the victim into divulging sensitive information, especially ATM card details. The attackers gain the victim's trust by calling out the first six-digit number IIN (Issuer Identification Number) of the bank ATM card which is a number that identifies the card issuing institution and is always the same for all customers. For example, GTBank's Naira MasterCard starts with '539983', UBA's Visa card starts with '492069', Access Bank's Visa card starts with '418745', and Zenith Bank's Visa card starts with '468588'.

✓ *Phishing*

It is the most prominent form of social engineering attack, it involves sending messages or emails that seem to be from a legitimate organization to the victims urging them to divulge sensitive information. The recipient might be prompted to fill out a form online or click on a link that will lead to a fraudulent site asking for personal information or downloading a malicious application. The attackers often use social media platforms to send out bulk phishing messages. Phishing attacks and other social engineering techniques, often exploit human vulnerabilities and behavioral tendencies to perfect their motives. Many phishing messages employ psychological triggers such as curiosity, greed, and fear of missing out (FOMO) to prompt recipients to click on malicious links or download harmful attachments. Additionally, the volume of Personally Identifiable Information (PII) individuals made available on social media platforms has provided cybercriminals with valuable insights into their interests, relationships, and preference data from which they can better tailor social engineering attacks to increase both credibility and persuasiveness.

Examples of phishing messages to bank customers in Nigeria.

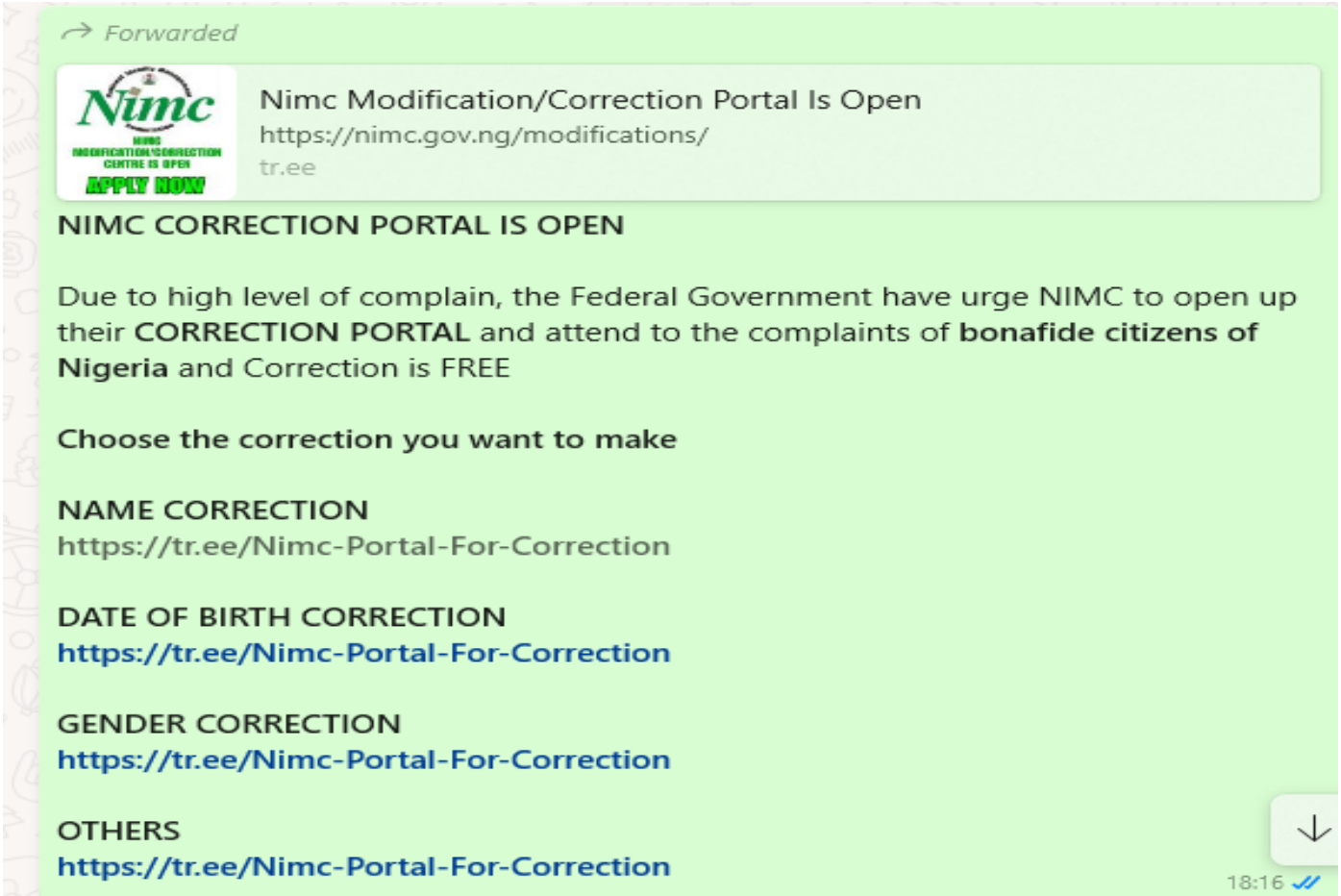

Fig 1 Fake NIN Modification Portal
Source: Whatsapp Groups

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

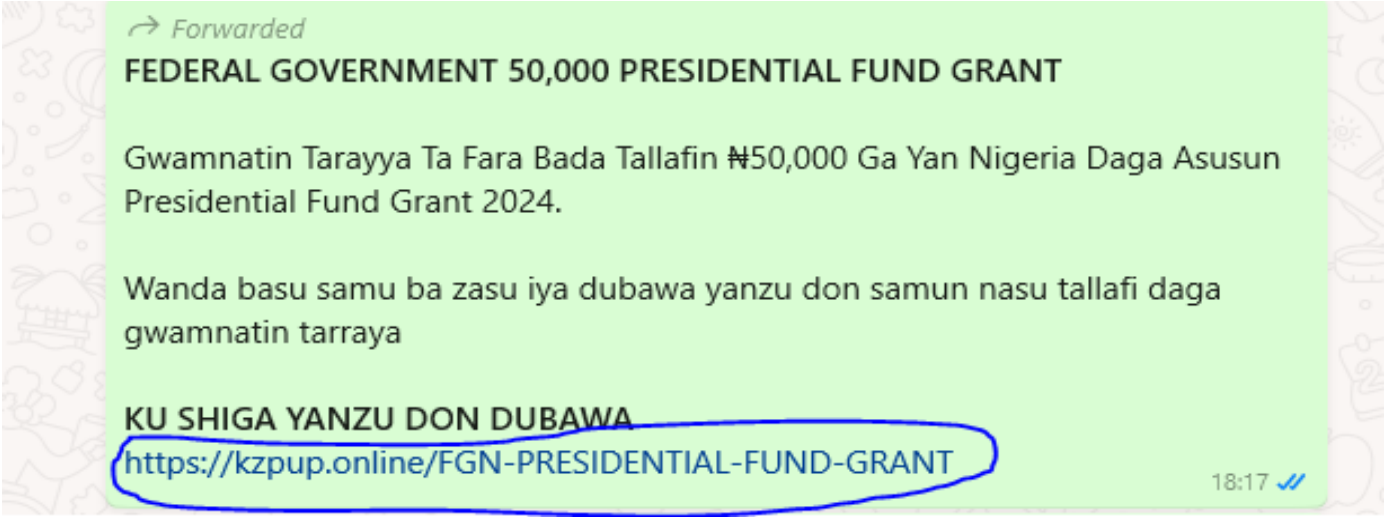

Fig 2 Fake Presidential Support Program
Source: Whatsapp Groups

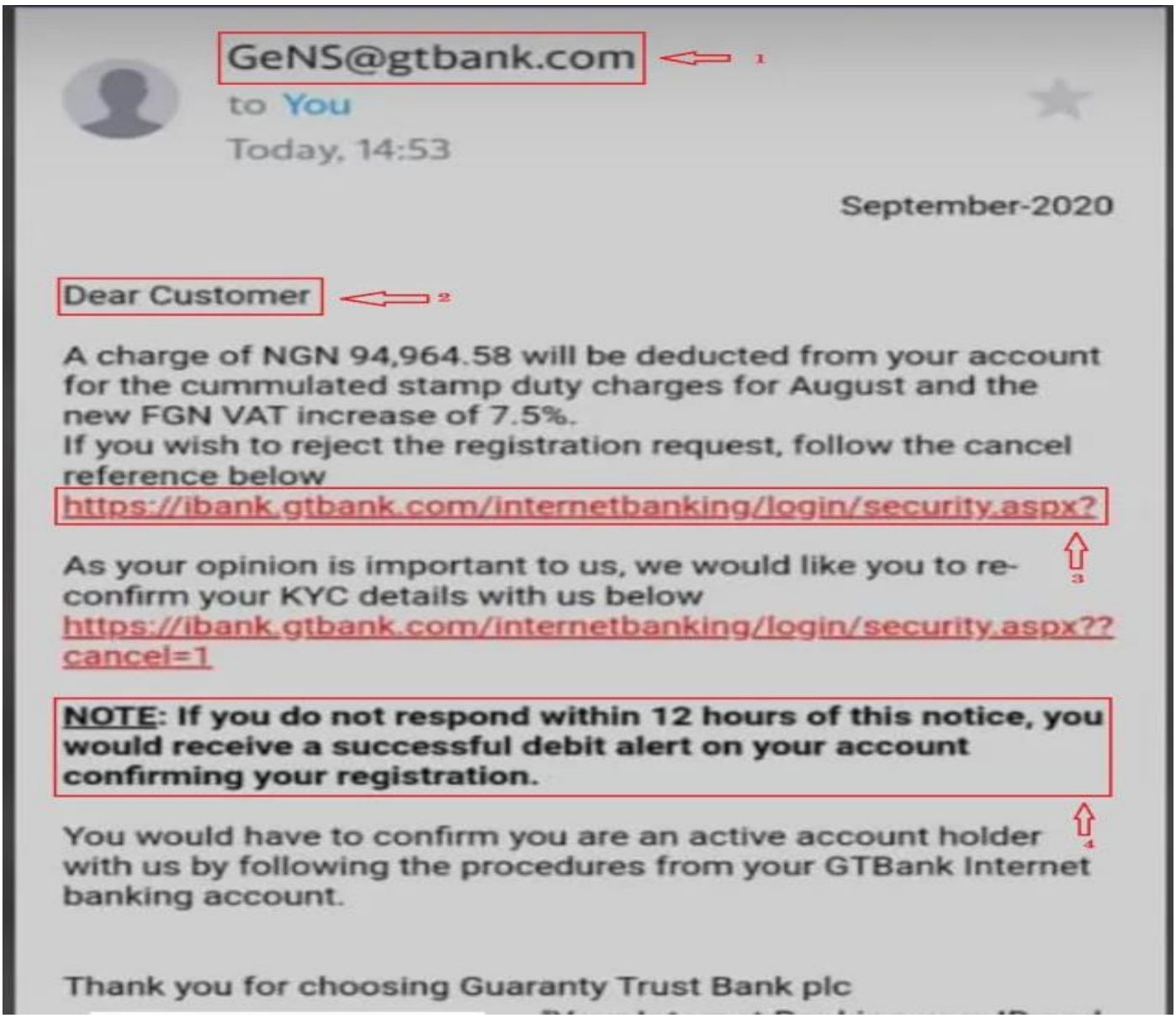

Figure 3. GTBank Phishing mail sample.
Source: Internet

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

- *Business Email Compromise (BEC)*

This is a type of cyberfraud in the banking sector where the attacker targets the business and individuals by gaining access to the Email linked to their account to defraud them. This type of attack usually depends on social engineering techniques and also when customers use the email linked to their account at random social media platforms or random online forms.

BEC also involves Fraudsters sending targeted emails to employees, business partners, or customers. The recipients, believing the emails are legitimate, then take actions that lead to fraudsters gaining access to sensitive data, funds, or accounts. Remarkably, most BEC attacks result in fraudulent wire transfers or financial payments.

- *ATM Card Swap and Skimming*

ATM (Automated Teller Machine) card swap is a type of fraud in which the scammer tricks the victim into exchanging their ATM Card and replaces it with a fake or expired one. In this technique, the scammers approach the victim at the ATMs point under the guise of rendering help or posing as a bank staff. After establishing the relationship, the scammer distracts the victim, either by engaging them in conversation, causing a commotion, or creating a sense of urgency. While the victim is distracted, the scammer swaps the victim's ATM card with a fake or expired one. The fake card often looks very similar to the victim's actual card to avoid immediate detection. In many cases, the scammer observes the victim entering their PIN during the distraction phase. They may use techniques such as shoulder surfing or installing hidden cameras at the ATM. The fake card usually got trapped by the machine making it easy for the fraudster to escape the scene and perform a withdrawal elsewhere.

✓ *Skimming*

Skimming, on the other hand, is a type of fraud that uses small digital devices called skimmers to record ATM card information such as PAN (Primary Account Number) digits and CVV Card Verification Value). The device is usually attached to ATMs and Point of Sales (POS) terminals allowing the fraudsters to obtain customer card information including PIN. The introduction of wireless technology makes it easier for criminals to download stolen data remotely without visiting a terminal.

Fig 4 ATM Card Skimmer.
Source: https://www.nwcu.com/learn/how-spot-atm-skimmer

➢ *Impacts of Cyberfraud in the Banking Sector*

Cyberfraud remains a significant threat in the banking sector globally, Nigeria inclusive. Its impact on the banking sector is not limited to customers only as it also affects the banks, economy, and country's reputation. Below are some of the impacts of cyberfraud in the banking system.

- *Financial Loss:*

Customers lose a substantial amount of funds in their bank account to cyberfraud, and the recovery effort for the fund lost also involves additional spending to obtain a court order as part of the requirement for a chargeback. The loss in the banking sector surged to 17.6bn in 2023 (NIBSS, 2023).

- *Emotional and Psychological Impact*

Individuals who fall prey to cyberfraud often suffer from significant stress and anxiety concerning their financial security and the safety of their data. Issues with emotional repercussions of fraud can result in a widespread distrust of digital banking and technology causing consumers to become hesitant about engaging with online banking services in the future.

- *Reputational Damage*

Reputation is the greatest asset of every bank as it is the weapon they use against competitors. Incidents of cyberfraud can undermine customer's trust and tarnish a bank's image which can result in the loss of business and the economy. Cyberfraud also affects Nigeria's reputation as it is one of the leading crimes to rate Nigeria among the top 5 countries with the highest rate of cybercrime in the world. (Oxford, 2024).

III. RESEARCH DESIGN AND METHODOLOGY

This study is conducted based on specific criteria pertaining to cyberfraud. Firstly, it is based on recent research, particularly focusing on the year 2023, ensuring that the information is both current and relevant. Secondly, the data utilized in this research were gathered from secondary sources, including various reputable outlets such as journals, books, NIBSS Annual Fraud Landscape, Annual statistical bulletin of the Central Bank of Nigeria, Commercial Bank reports, and websites. This approach was taken to guarantee the authenticity of the collected information. Lastly, the research specifically centers on cyberfrauds aimed at customers.

IV. RECOMMENDATION

This research reveals the major techniques employed by fraudsters in scamming bank customers in Nigeria. The fig1. above is a phishing message disguised to assist individuals with the NIN (National Identification Number) issue. However, clicking on the link will redirect the user to a different website created by the fraudsters aiming to steal the victim's data including their bank credentials details that can be used to launch cyberfraud on them.

The figures below indicate the analysis of the link to the phishing and it leads to the portal

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

https://wjdwswsowsdwxwdw.blogspot.com/

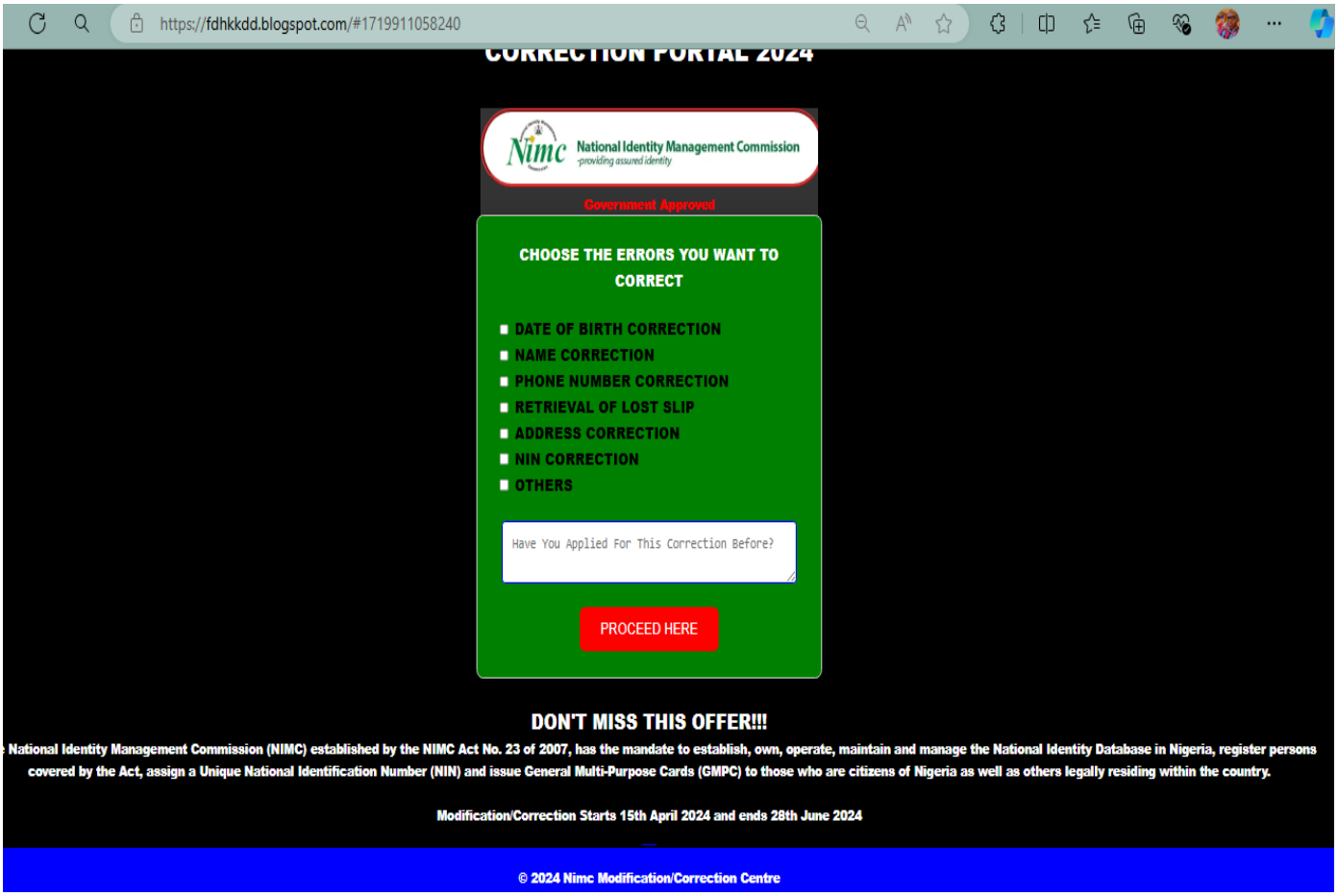

Fig 5 Fake NIN Website

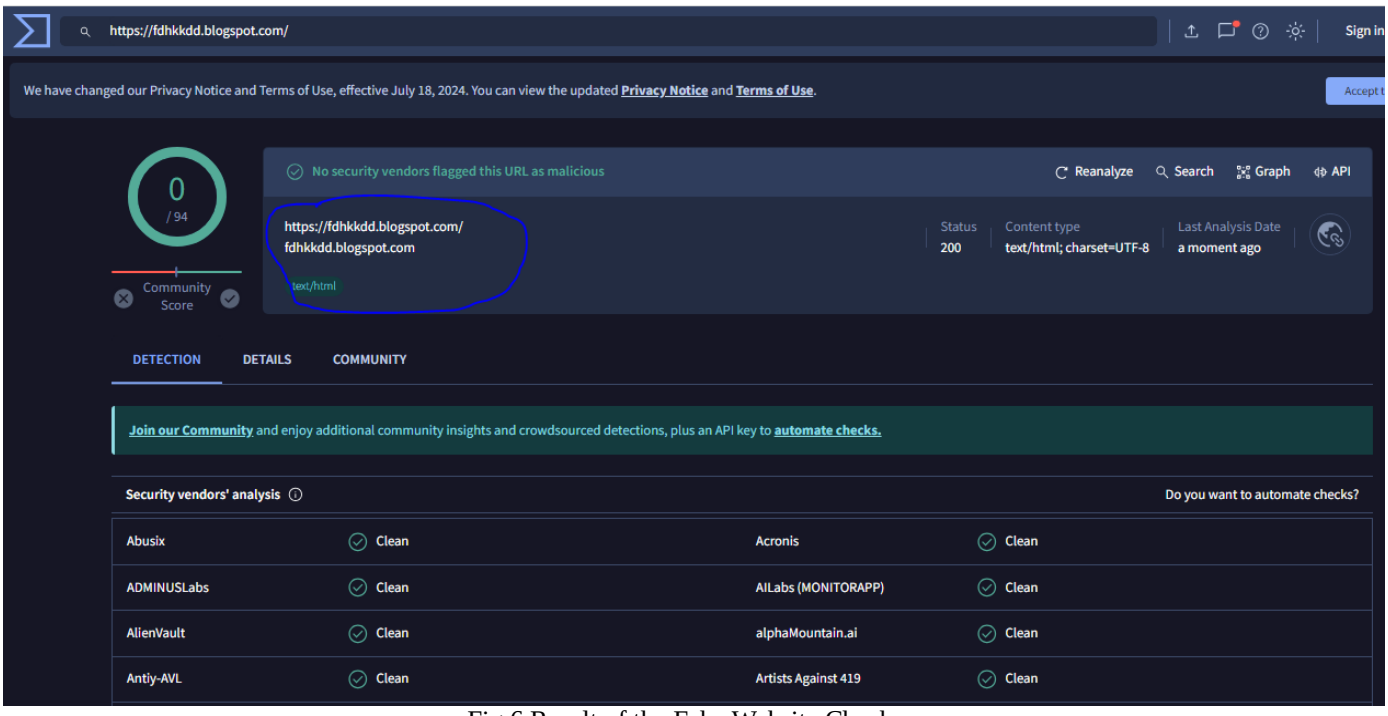

Fig 6 Result of the Fake Website Checker.

The fig 6. Is a result of the fake website checker. However, the result recognizes the website as clean this is because no security vendor had reported the link as malicious.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

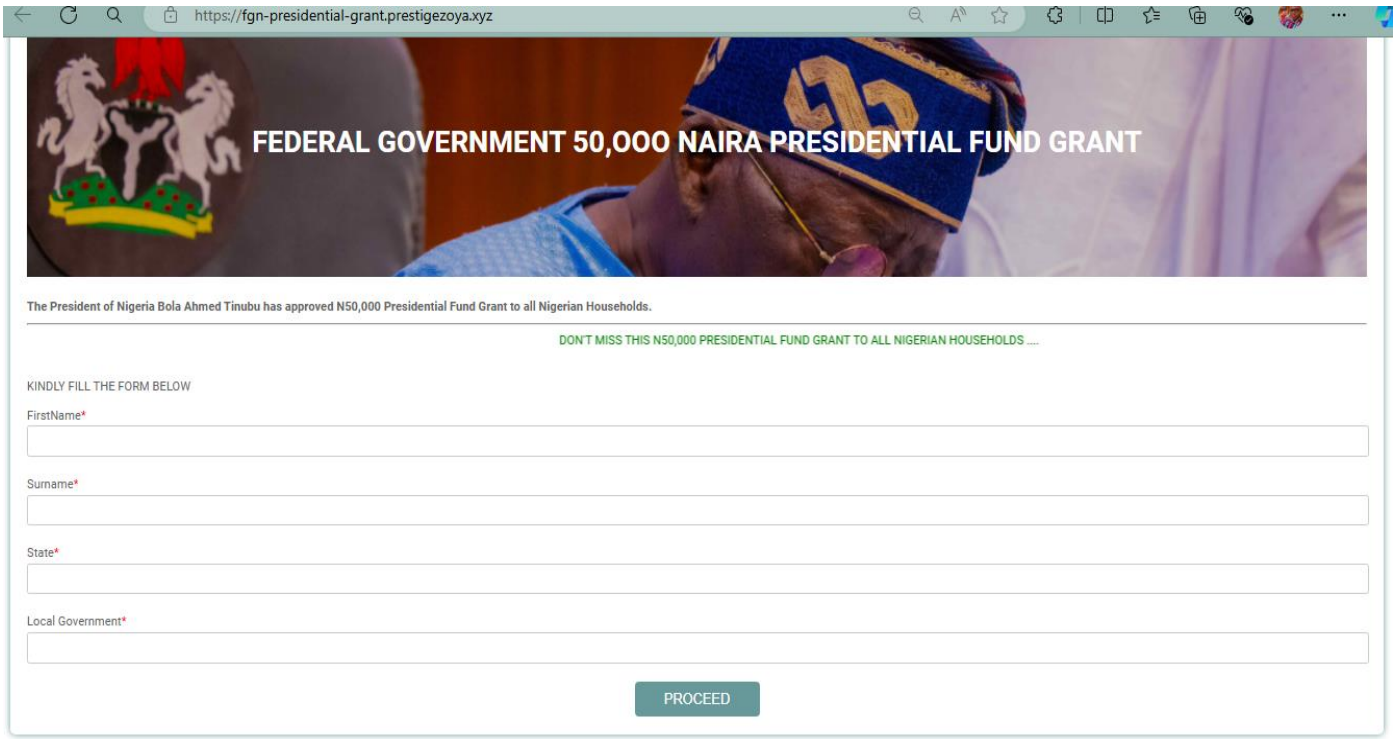

Fig 7 Landing Space of Fig 2.

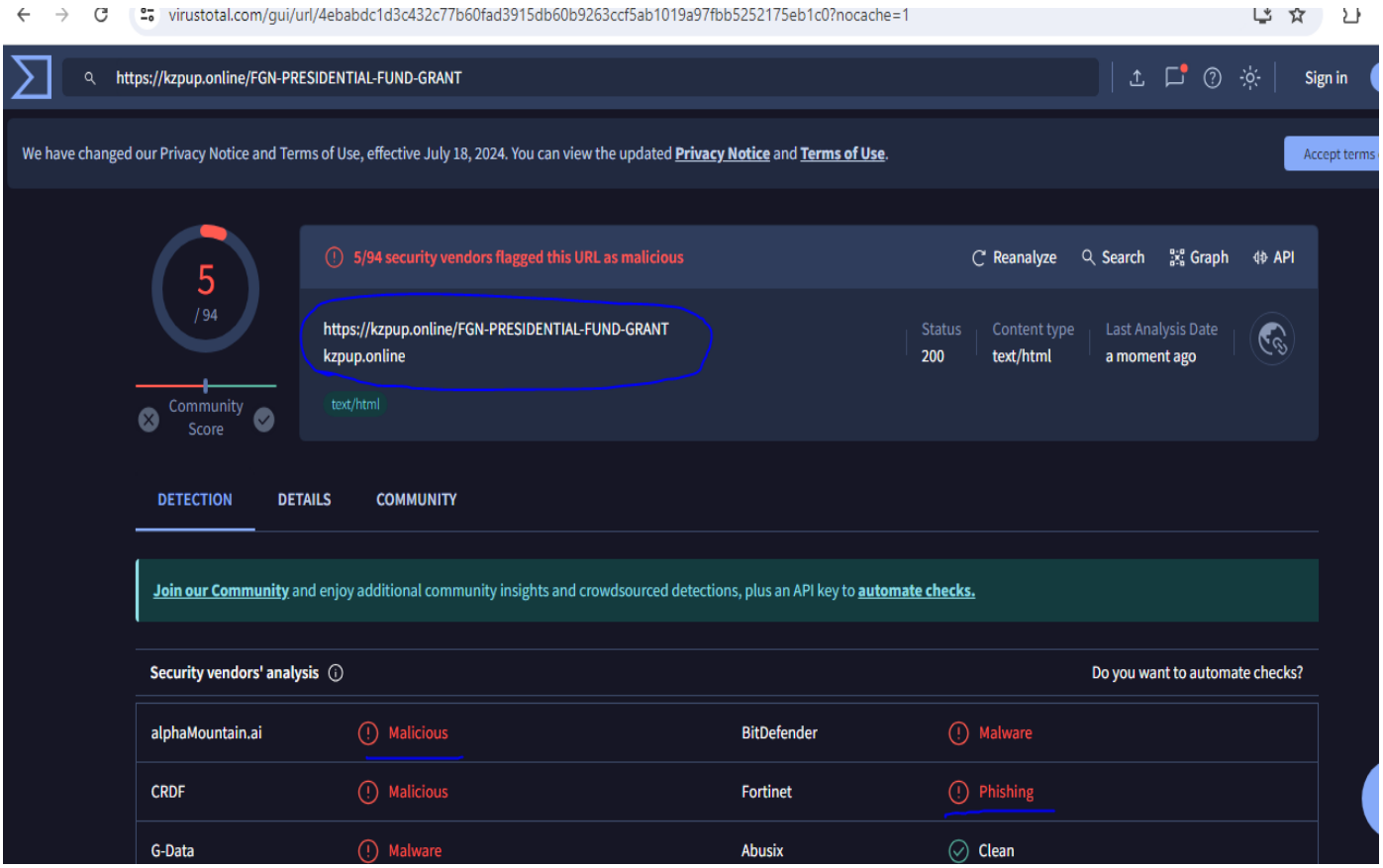

Fig 8 Result of Fake Website Checker.

The findings of all the phishing message samples indicate that they usually lead a victim to a fraudulent portal designed for data theft. Those data are used to launch attacks either instantaneously or later on to avoid suspicion.

Forbes in an article published on their website on 29th April 2024, concluded that there is a high rate of youth involvement in cyber fraud in Nigeria. And people of aged 40 and above are more vulnerable to cyberfraud (NIBSS, 2023)

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

There are essentially two different types of security strategies: raising user awareness and making use of additional programmed tools. (Baballe, 2022). There is no standard defensive measure for Social engineering attacks due to its evolving techniques and no individual is totally free from social engineering attacks.

"Don't assume it can't be you. No matter what you do for a living, or where you are in your life or how efficient you think you are—nobody is above being scammed." **– Lilah Jones on Business Email Compromise Scams.** (Nasdaq & Verafin, 2023).

"People always think it could never happen to them—I know I did, and I'm a former intelligence officer. If it can happen to me, it can happen to anyone."-**Debby.** (Nasdaq & Verafin, 2023).

However, it can be minimized to the bare minimum by creating adequate awareness about its modus operandi.

Below are some recommended preventive measures to be adopted in combating cyberfraud in the banking system.

➢ *For the Government:*

- Increase the rate of employment among youths in the country.
- Strengthen the implementation of cybercrime penalties.
- Create more awareness on how to report cyberfraud incidents on the NPF(Nigerian Police Force) portal https://incb.npf.gov.ng/
- Make a regulation for POS operators to keep track of all users by using CCTV and obtain a valid means of identification for high amount withdrawal.
- Provide funding for creating cyber awareness in National dailies and media houses.

➢ *For the Banks.*

- Educate customers and their staff about cyberfraud techniques during the onboarding process.
- Increase the fraud management team to enable swift action for fraud reported cases.
- Enforce multifactor authentication for mobile banking to prevent mobile app switching.
- Use Emails, SMS, and in-app notifications to alert customers about potential threats and provide tips for secure online behaviour.
- The CCTV cameras around ATMs should be properly positioned for effective footage.

➢ *For the customers*

- Be sure to download Apps from reliable app stores like Google Play Store and Apple App Store.
- Review app permissions and avoid granting unnecessary access to personal data.
- The personal information shared on social media platforms should be limited.
- Be aware that banks don't request personal information via phone.
- Customers should be cautious of unsolicited SMS, Emails, or calls asking for sensitive information or requesting urgent action.
- Always verify the source of the message before clicking on links or divulging information.
- Avoid using Emails attached to the bank account on random sites.
- Enable multi-factor authentication, i.e. a combination of password and biometrics.
- Avoid using the same password across multiple accounts.
- Stay vigilant when operating ATMs and seek assistance from bank staff when necessary.
- Avoid having your ATM card out of sight at the POS centres.
- Stay up-to-date about the trending cyber threats and practice online safety.
- Be familiar with account restriction codes, and report any fraudulent activities to your bank.

V. CONCLUSION

The banking sector contributes eminently to the economic stability of the nation. The nature of its operation in providing financial services makes it and its customers a consistent target for fraudsters. The sector's sustainability hugely depends on the level of confidence the customers have in it. This level of confidence has been marred by the issue of cyberfraud. This study aimed to identify the techniques, impacts, and preventive measures for cyberfraud incidents targeting bank customers.

This study recommends that combating cyberfraud in the banking sector is a collective effort, the banks, law enforcement agencies (Government), and customers have to contribute their quota in mitigating cyberfraud to the barest minimum. Adopting the preventive measures recommended in this research will contribute greatly to achieving the goal of maintaining the integrity of the sector, the country, and safeguarding the customer's fund.

REFERENCES

[1]. Alhaji, K., & Simon, F. (2018). Fraud Prevention in the Nigerian Banking Industry. *IIARD International Journal of Banking and Finance Research*, 32.

[2]. Brush, K., & Kobb, M. (2024, January). *https://www.techtarget.com/searchsecurity/definition/cybercrime*. Retrieved from www.techtarget.com: https://www.techtarget.com/searchsecurity/definition/cybercrime

[3]. CBN. (2023). *Annual Statistical Bulletin.* Central Bank of Nigeria CBN.

[4]. Fortra. (2024, July 26th). *Social Engineering Attacks: Common Techniques and How to Prevent Them.* Retrieved from https://www.digitaldefense.com: https://www.digitaldefense.com/blog/social-engineering-attacks-common-techniques-and-how-to-prevent-them/

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG395

[5]. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* . Indiana: John Wiley & Sons, Inc.
[6]. Kyrychenko. (2021). Fraud in the banking system of Ukraine: ways to combat taking into account foreign experience. *Amazonia Investiga, https://doi.org/10. 34069/AI/2021.45.09.21*, 208-220.
[7]. Nairametrics. (2024, April 26). *nairametrics.com*. Retrieved from nairametrics.com: https://nairametrics. com/2024/05/08/cbn-official-list-of-deposit-money-banks-in-nigeria-as-of-april-2024/#google_vignette
[8]. Nasdaq, & Verafin. (2023). *Global Financial Crime Report*. USA: Nasdaq, Inc.
[9]. NIBSS. (2023). *The Annual Fraud Landscape.* Nigeria Inter-banks Settlement System NIBSS.
[10]. Olumayokun, A., Adewumi, A., & Oluseyi, O. D. (2023). Bank Verification Number and Fraud Prevention and Detection in Nigerian Banks. *https://www.rsisinternational.org/journals/ijriss/*.
[11]. OpenAI. (2024). *ChatGPT*. Retrieved from https:// chatgpt.com/: https://chatgpt.com/c/1e6e90bc-6467-4a88-ac83-958d49013fc4
[12]. Oxford, U. o. (2024). *https://www.ox.ac.uk/news/2024 -04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level*. Retrieved from https://www. ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level: https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level
[13]. Wingard, L. (2024). *Hitachi Solutions.* Retrieved from Global Hitachi Solutions.: https://global.hitachi-solutions.com/blog/fraud-prevention-in-banks/Fraud. 2024. In *Merriam-Webster.com.*
[14]. Retrieved July 22, 2024, from https://www.merriam-webster.com/dictionary/fraud