International Digital Organization for Scientific Research
IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES 7(1):25-32,2022. ISSN: 2579-0803

Social Engineering Attack, Its Effects and Countermeasures in Nigeria Banking System

[1]Chika Lilian Okafor, [2.]Obi Okonkwo and [3]Uchenna Paulinus Onwuka
Department of Computer of Computer Science NnamdiAzikiwe University, Awka, Nigeria

ABSTRACT

Banks in Nigeria are faced with numerous social engineering -attacks, this has led to huge financial and valuable loss. The introduction of electronic banking has widening the gap of intruders into the system with the help of internet of things. The increasing rates of cybercrime in Nigeria has become a strong threat to Nigeria's banking system, despite the security measures put in place to subdue and protect customer's finances and information. Commercial banks remain the most targeted financial institutions/businesses for cyber hackers or cybercriminals. Ever since the evolution of banking, there have always been a number of unscrupulous individuals who have tried to breach its defenses in order to gain access to valuables. In the course of time, the physical attacks have become slowly less necessary because banking has steadily gained an online presence. Formerly, it was impossible to authorize a transaction through a mobile phone using the Internet. However, now that is more than possible, it is an extremely popular way of having transactions. As a result, security within financial institutions has shifted focus from physical to virtual measures. This research review social engineering attacks and its effect in Nigeria Banks, and also suggest some measures to counter the attack.

Keywords: Cybercrime, internet banking, commercial banks, hacker, Nigeria, cybercriminals, financial institution.

INTRODUCTION

In Nigeria, modern Internet banking evolved so fast, bringing enormous relief to the complex banking operation and service rendered in the late 90's [1,2,3,4]. Nigeria's banking industry witness it's first huge transformation after the Structural Adjustment Program introduced by the former President of Nigeria Ibrahim BadamosiBabangida in 1986 , commercial banks increased in number from 40 – 125 in 1991, staff strength and services, making it necessary for the institution to improve the strategies to better its services [5,6,7]. Across the world, cybercriminals have long been using phishing and other social engineering methods to trick their victims into providing access to confidential data, such as passwords, social security numbers or account numbers [8]. The introduction of the internet banking system has added value to the banking system in Nigeria, bringing services like online transfer, payment, and mobile banking, sematic data warehouse, automated teller machine, electronic fund transfer, point of sale, and electronic cheque, other after sales services [9]. Nigeria has the highest number of internet users and mobile subscribers in telecommunication in the world, which has aided the patronage to internet banking [10]. However, it has attracted the activities of hackers/cybercriminals. Cybercrime (computer-crime) is any illegal act targeted by means of electronic operations on the security of computer systems and the data process of them [11]. Cybercrime now has a growing trend affecting the financial sector in the form of credit card fraud, automated teller machine scams, identity theft, website phishing, denial of service attack [12]. The banking sector and financial institution are one of the sectors abruptly affected by cybercrime in Nigeria, despite the legal and security measures put in place to curb this menace [13]. In Nigeria, the Central Bank of Nigeria (CBN) recently disclosed that social engineering has become rife in cybercrime attacks in Nigeria. According to the central bank, almost on a daily basis, a plethora of messages are sent by these criminals with the express intent to scam the unsuspecting recipient using techniques that appeal to vanity, greed or authority [14].Since Nigeria Banks has gained

much online phase, security of financial transactions should be given much attention and it is a very important issue that needs to be addressed very carefully, as online banking is one of the most sensitive tasks performed by general user [15].Therefore, the banking sector regulator stressed the need to look critically at measures that will protect the industry as a whole from the menace of social engineering attacks. This paper will examine social engineering attack and how it is affecting Nigeria banking system, andsuggest the countermeasures.

Background

Commercial institution in Nigeria has metamorphosed positively over the years to compete with international business standard, one of the reforms after the structural program of 1986 that consolidated the system is the 2005/2006 merger and closure that sliced the numbers of banks from 125 to 26 lucky N25 billion minimum shareholders' funds for Nigeria deposit with banks [16]. The major role of Nigerian banking system is to facilitate financial transaction, keep customers information/records safe, offer other financial related services, and provide security where needed. The internet is the global presence that connects many computers (banking sectors) and users of the internet, for the benefit of sharing vital information among themselves [17]. Internet technology is one major medium that has ease customers satisfaction, but came with security challenges which calls for worry by both banks and customers in Nigeria.Almost all banking system now uses a centralized banking application to run its daily operations from the head office, under the supervision and monitoring of the apex bank Central Bank of Nigeria (CBN) across it branches. Banking is now made easy as customers can now perform transactions from the comfort of their homes, using mobile banking application, codes and other after sales services. Shifting to the centralize control of financial management, share of information and customer services in Nigerian banking system has increased the number of computer crime and prospective offenders, making it difficult to trace, detect and prevent these crimes. However, the growth of online banking environment is accompanied by new and existing threats. Several cyber-attacks are meted on financial institution to cause great harms in new and critical ways, some of which are online fraud and internet spoofing. According to Ogunlere ,Cybercrime has not only affected the financial institution in Nigeria, it has also discourage foreign investors from investing in Nigeria [8]. Commercial banks in Nigerian loses over NGN 15 billion (US$39 million) in 2018 to cyber-crime and electronic fraud, thereafter an increasing rate of cyber fraud, customers deposit lost have been recorded to the sum of NGN 1.9 billion on a yearly basis [11]. In order to curtail this, banks employ the services of cyber experts to help manage their cyber security challenges, build intense firewalls, implement strong authentication control, train bank staff on security measures and improve physical security within the banking facilities. The government has also taken corrective measure by setting up the National cyber security initiative (NCI) in 2013 and Nigeria cybercrime working group (NCWG), which unfortunately did not meet up with the rate of growth cybercrime.

STATEMENT OF THE PROBLEM

There has been a global campaign against the growing threat of cyber-crime onSome of the extract from research papers explains the challenges commercial banks faces from cyber-crime in Nigeria as follows:

- SanusiLamidoSanusi former governor of the Central Bank Nigeria in one of his reforms while in office affirms that losses in some commercial banks amounting to 70% as a result of fraudulent Internet hacker's activities eventually lead to the closure of some banks due to the magnitude of losses they encountered.
- Access Bank a commercial bank in Nigeria denied been hacked, despite the fact that well renown hacker's like Ihebuzo Chris claimed to stumble on sensitive customer data from the bank database.

- On August 25, 2020, a hacker via twitter handle posted that he has small dump of a database (containing PII) belonging to Unity Bank Nigeria, which was later confirmed by the Bank Security.
- Team-Apt also claimed that only a snapshot of their source code was released by hackers.

Theoretical Review

Nigeria Banking System

The origin of institutionalized banking in Nigeria started sometime in 1883 with the establishment of the African Banking Corporation. This was quickly followed up by the establishment of the British Bank of West Africa in 1884. The African Banking Corporation failed shortly after its formation, while the British Bank of West Africa has evolved into the oldest bank in Nigeria today, the First Bank of Nigeria. The British Bank of West Africa over the years changed names at different periods; initially to standard bank West Africa, standard bank of Nigeria and presently, First Bank of Nigeria PLC. Other financial institutions in forms of banks followed suit soon including the precursors of the present-day union bank of Nigeria PLC. Owing to the fact that these banks were established to protect the interest of their foreign owners, the policies of the banks were rather discriminatory against the very indigenes who, being denied credit advances in these banks, became effectively excluded from the mainstream of the economy. The resultant alienation ignited the protagonist of the nationalist of the wholly indigenous banks in Nigeria. Thus, for the periods spanning 1929 and independence in 1960 nothing less than 26 such banks were formed out of which only four survive till present day. However, with the liberalization of licensing of banks following the introduction of Structural Adjustment programme (SAP) in the second half of 1980s, the scope of banking in Nigeria expanded both in size and operation. According to [7] this development heightened the rate of competition among banks. The level of competition has been further intensified in this century because of the effect of globalization and integration of the banking industry into the global economy. Consequently, management of Nigeria financial institutions are faced with tremendous challenges and should brace up to these challenges. Thus only those institutions that are well positioned will become relevant and will be able to withstand the storm of Challenge.

Social Engineering Attack

In the context of computer and cyber security, social engineering describes a type of attack in which the attacker exploit human vulnerabilities by means such as influence, persuasion, deception, manipulation and inducing, so as to get classified information, hack computer system and network, obtain unauthorized access to restricted areas, Social Engineering Attacks According to Christopher [6], the term social engineering is defined as “the act of manipulating a person to take an action that may or may not be in the target’s best interest. In contrast to this definition, [8] describes social engineering as “a euphemism for non-technical or low-technology means—such as lies, impersonation, tricks, bribes, blackmail and threats used to attack information systems” The descriptions above provide an insight into how social engineering attacks rely purely on the human factor. An attacker may use human behavior as a tool to attack information systems by manipulating an unsuspecting target. Social engineering attacks are multifaceted and include physical, social and technical aspects, which are used at different stages of the actual attack. This section presents an organized account of common maneuvers, strategies and tactics used in social engineering attacks. In hacker community, social engineering is a quite popular attack since 1970s [9]. Compared to classical computer attacks such as password cracking by brute-force and software vulnerabilities exploit, social engineering attacks focus the exploitation of human vulnerabilities, to bypass or break through security barriers, without having to combat with firewall or antivirus software by deep coding. In addition, there is not a computer system doesn’t rely on humans or involves

human factors on earth, and these human factors are obviously vulnerable or can be largely turned into security vulnerabilities by skilled attackers. These inevitable and vulnerable human factors makes social engineering to be a universal cyber security threat. For some situations, social engineering attacks may be as simple as making a phone call and impersonating an insider to elicit the classified information. Moreover, with the development of new technology and the formation of new cyber-environment, social engineering threat is increasingly serious. Social Network Sites (SNSs), mobile communication, Industrial Internet and Internet of Things (IoT) generate not only large amounts of sensitive information about people and devices but also more attack channels and a bigger attack surface. Unrestricted office environment (bring your own device, remote office, etc.) leads to the weakening of area-isolation of different security levels. The Chief Executive Officer of Sterling Bank Plc, Mr. YemiAdeola, said fraud remains a major concern to banks and financial institutions worldwide, adding that Nigeria is not an exception. According to him, the introduction and advancement in electronic payment system in the Nigerian financial system came along with significant challenges associated with this kind of innovation."Thousands of Nigerians have fallen victims and several billions of naira lost to the activities of these fraudsters since the introduction of e-payment system. Statistics available to banks and law enforcement agencies shows that this challenge is still on the increase. Most of the information used by these fraudsters are gotten from social engineering attacks.

The Attack Cycle

The social engineering attack process was first described by Kevin Mitnick. He described it as an attack cycle of four phases [7].

1. Research: This involves gathering information about the target. The final result is dependent on the quality of the information collected at this stage. The data collected is utilized in succeeding phases and is of crucial importance in making the attack successful.
2. Developing Rapport and Trust: Various types of social engineering techniques are deployed in this phase to ensure the victim trusts the attacker. The data collected in the first phase, such as public name, employer's details, and company details, are used to make the victim believe they are truly dealing with the organization.
3. Exploiting Trust: Attackers manipulate human behavior and exploit trust and stealthily steal the desired information. This can be executed in multiple ways, for example email spoofs, scam phone calls, or malware installation.
4. Utilize Information: This final phase is also referred to as "cashing in", where the information gained from the previous phases is used to perpetrate the attack.

Various researchers have presented variants of Mitnick's social engineering attack cycle, providing description variants and extensions. Since social engineering attacks essentially exploit an information system by gathering details of individuals or organizations, According to Software Engineering Institute, USA publication in 2014, the exploitation can be a single-stage or multi-stage attack.

- Single-stage attack: As the name indicates, the attack is performed just once.

The informationCollected is utilized to exploit the users' financial transactions for fraudulent purposes.

The single-stage attack ends after conducting the attack only once.

- Multiple-stage attack: A multiple-stage attack occurs when the information collected from a Successful attack is used to deploy one or more similar social engineering attacks. The time duration of multiple-stage attack can be minutes, hours or even weeks or months. This dependson the nature of the threatened person and/or the organization involved.

ATTACK VECTORS

An attack vector is a path or means by which the attacker can gain access to exploit system vulnerabilities, including the human element.

Social Approach

The attack vectors in social approach can be arise through different acts, tailgating, impersonating, eavesdropping, shoulder surfing, dumpster diving, reverse social engineering and others.

Tailgating

Tailgating is the act of following an oblivious human target with legitimate access through a secure Door into a restricted space. The attacker may ask the victim to hold the door, or can simply reach forit and enter before it closes. Considering that in the recent past, safety and health regulationsProhibit smoking in company premises, this is an increasingly e effective technique as it providesOpportunities for social engineering to tailgate groups of smokers.

Impersonating

As the name implies, the threat actor assumes a false identity to gain credibility as a basis to carry outfollowing malicious actions, like piggybacking, pretexting and quid pro quo. Piggybacking, similarly to tailgating, the attacker aims to gain physical entry to secured areas. In this case however, acquires permission from the person with legitimate access by impersonating businessentities, like personnel that require temporary admittance.

Pretexting

The core of this attack is the fabrication of a plausible scenario propitious to engage the targeted victim. Impersonating an authority figure or a trustworthy entity, the attacker attempts tobreach security protocol and gain access to credentials and personal information. This method requires a credible story to prevent arousing suspicion, and thus conducting research on the target isabsolutely necessary.

Eavesdropping

Within a company, the personnel may simply discuss classified matters out loud if expecting only authorized employees to be present. Just for being at the right place at the right time, threat actors canexploit security breaches of this nature. Nevertheless, attackers can also pro-actively listen to Communicating channels such as e-mails and telephone lines.

Shoulder surfing

Refers to the act of direct observation by surfing over the victim's shoulder to collect personal Information, typically used for extracting authentication data.

Dumpster diving

A classical practice for acquiring sensitive information among attackers is to simply look for it throughthe garbage. Often, individuals and organizations, do not adequately dispose of documents, papersand even hardware from which can be retrieved confidentialdata.

Reverse social engineering

The threat actor entices the target to be the one to initiate the interaction and lies in wait, reducing therisk of arousing any suspicions. The attacker creates and plays a persona that appears to be trusted,fabricates a problem for the victim and, indirectly, presents a viable solution.

A Recurrent Social Attack Example

In 2015, astute cyber criminals used vicious social engineering tactics to ruthlessly attack and bypasstwo-factor authentication systems. By exploiting the public trust in a credible entity, one attack wasnotably successful, the Gmail scam. A recurrent social attack example in six steps. First step, an attacker extracts the target's email address and phone number through research, often with ease. Second step, the threat actor initiates the attack by sending a message to the potential victim via SMS44, equivalent to: "Google has detected unusual activity on your account. Please respond with the code sent to your mobile device to stop unauthorized activity." Third step, the attacker, impersonating the victim, requests a legitimate password reset from Google. Fourth step, Google sends the password reset verification code to the actual victim. Fifth step, the victim, expecting the message from Google,

follows the previous instructions and forwards the code to the attacker. Sixth step, with the code, freely given by the victim, the attacker simply resets the password and gains complete access to the account. After accomplishing the purpose of the attack, simply informs the victim of the new temporary password, terminating contact without arousing any suspicions.

Socio-Technical Approach

The social-technical approach can be arise through different situations, phishing, baiting, fraudulent websites, vishing etc.

1. Vishing: Vishing is a form of social engineering attack in which an attacker uses a phone call totrick a victim to reveal sensitive information such as credit card number, pin code or detailed home address. The attack exploits voice over IP (VoIP) technology since it is cheap, and the attacker could be calling from anywhere around the world, with their identity concealed [8].

2. Baiting/Trojan Horse: Baiting uses digital devices such as USB drive or RAM to gain a victim's attention and perpetrate an attack. This technique relies on human curiosity to deploy the attack, which in turn spreads the malware installed on their device. As a result, the organization's Internal network will fall under the control of the hacker.

3. Fraudulent Websites: With this attack type, the hacker exploits a victim's trust, leading themto access their fake website, which automatically downloads malicious files onto the victim's computer[7]. As with the Trojan horse attack, the downloaded file gives the attacker access to sensitive information from the local browser of the victim.

4. Pretexting: This is an exploit that uses a scripted scenario to trick the victim to reveal sensitive Information or accomplish other malicious activities unknowingly. Reverse social engineering is the best example for pretexting, in which an attacker creates a scene or situation and an innocent Victim believes that the hacker can provide a solution.

5. Phishing/Spear Phishing: Phishing is the most popular social engineering attack in the online banking system. Typically, a hacker sends an email using the legitimate organization's trademark to get the attention of their target. The fake email appears to be from a trusted bank requesting that the customer updates their account information using the provided link (which is a bogus link). The attached fraudulent website leads the victim to divulge sensitive financial credentials. Phishing is considered one of the most effective attacks and the technique has become more sophisticated over the years. Spear Phishing uses the personal details of a potential victim to tailor the email content, with a higher probability of success [5].

Effects of Social engineering attack on Nigerian Banks

Huge financial loss

Due to the rising of electronic transactions, bank customers recorded a loss of N5.02 billion between January and September 2020 in 41,979 fraud-related incidences representing 91 percent success out of the total 46,126 fraud attempts. This is according to data at the Nigeria Inter-Bank Settlement System [7] shown in its latest report titled Fraud in the Nigerian Financial Services. The data also showed N203.357 million were partially lost by customers in 984 fraud attempts while 3,163 fraud attempts were repelled that could have resulted in the loss of N380.159 million. A breakdown of how the frauds were perpetrated in 2020, shows majority of the fraud was done via the web representing 47 percent, Mobile transaction 36 percent, Automatic Teller Machine 9 percent while internet banking 1 percent. On the yearly growth, Mobile channel rose by 330 percent, while Web and Point of Sales channels fraud activities increased by 173 percent and 215 percent respectively from 2019 to 2020. During the first 9 months of 2020, July represented the biggest loss for customers, as over 7,000 fraud cases were recorded. January and March followed behind with over 5,000 fraud attempts in volumes. On the technique applied to defraud bank customers in 2020, NIBSS revealed that Social engineering remains one of the principal ways in which fraudulent activities are attempted. Social engineering is a way of manipulating a victim into giving away sensitive information. NIBBS

disclosed that 56 percent of fraud techniques were Social engineering, followed by phone theft, card theft and fake assistant representing 6 percent. PIN compromise was 3 percent of the total fraud activities, Robbery 2 percent, Lack of 2FA 1.9 percent, missing lost card 1 percent, card phone theft 1 percent [8].

SOME INCIDENCE OF CYBER CRIME ON NIGEIRA COMMERCIAL BANK

- In 2019 the Apex bank (CBN) confirms that transaction values at N6.5 trillion was stolen by hackers on commercial banks in Nigeria. Nigeria Inter-bank System (NIBSS) states that between 2014-2018 commercial banks have lost over N12.30 billion to internet fraud in Nigeria.
- Recent report says that point of sale (POS) might be susceptible to data breach as a result of its global growth. In 2013, a Trojan POSRAM malware was used to steal payment card information of about 70 million customers belonging to a retail giant, banking with a commercial bank in Nigeria. (African Academic Network on Internet.

Countermeasures to Social Engineering Attacks on Nigerian Banks

- Set up an Anti-Scan Centre in the geopolitical zone in Nigeria, in alliance with other international anti scam centers, to impede fund transfer and every other medium used by cybercriminals to perpetrate crime.
- For investors and customers, simple security tips such as having and updated and original anti-virus software to avoid disclosing personal information to third parties. Using strong password and changing password at interval, ignoring emails request financials or person details to unblock accounts will help to prevent security breaches.
- use of Biometric Authentication such as finger print and face recognition with the OTP (One Time Password)
- Regular training of staff and IT officers of banks on the new technologies.
- Develop online games (Persuasive App) to create awareness to sensitize customers on the fraudulent activities of hackers.
- . CBN should implement a strong policy to integrate BVN (Bank verification Number) with Biometric Authentication during online /Mobile transaction.

CONCLUSION

Nigeria is rated high in its engage in cybercrime. The general public in its involvement in the evolution of the internet of things, used to promote the general services of the commercial banking system in Nigeria, it is paramount to note that cybercrime will become a common activity. So it is evidence that the government needs to improve its cyber security strategy, in order to preserve its image locally and internationally. A proper oversee and implementation of the cybercrime (Prohibition, Prevention, etc.) Act 2015 ("Act") will go a long way to curb and protect the rate of cybercrime in the commercial banks in Nigeria. Since computer crime cannot be totally subdued and eradicated from the banking sector, banks would have to be innovative to meet up with the growing trend of technology and security advancement. Going by this research, security measures if applied will curtail the intrusion from cyber criminals. Fighting cybercrime requires a general methodology to control the damage this menace will have on the financial institutions, businesses and nation in present and future term.

REFERENCES

1. Abu-Shanab, E.; Matalqa, S. Security and Fraud Issues of E-banking. Int. J. Comput. Netw. Appl. **2015**, 2,179–187.
2. Andrea Cullen, Lorna Armitage, "The social engineering attack spiral (seas). In Cyber Security And Protection of Digital Services (Cyber Security)", 2016 International Conference On, pp.1-6,IEEE, 2016.
3. Aburrous, M.; Dahal, H.M.A.K.; Thabatah, F. Experimental Case Studies for Investigating E

BankingPhishing. J. Cogn, Comput. **2010**, 2, 242–253.
4. E-Security Planet. Social Engineering Attack Nets $2.1 Million from Wells Fargo Bank; e-Security Planet Foster City, CA, USA, 2012.
5. Hadnagy, C. Social Engineering: The Art of Human Hackin, 1st ed.; Wiley: Indianapolis, Indiana, I.W. stats, "www.internetworldstats.com," InternetWorldStats, [Accessed August,2022].
6. ITU, "Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders," International Telecommunication Union, vol. A/CONF.187/10, p. 5, 2000
7. Katharina Krombholz, HeidelindeHobel, Markus Huber, Edgar Weippl, "Advanced social engineering attacks", Journal of Information Security and applications, Vol.22, pp.113-122,2015.
8. Mika Kontio et al, "Social engineering", pp.101, 2016.
9. M. Ogbonnaya, "Cybercrime in Nigeria demands public-private action," Senior Research Consultant, ISS Pretoria, 2020.
10. Nabie Y Conteh, Paul J Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures toprevent social engineering attacks", International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016. Nigeria, "History of e-banking in Nigeria," ifiokobonkibanga, 2020
11. Prashant Kumar Dey, "Prashant's algorithm for password management system", International Journal of Engineering Science, pp.2424, 2016.2010.
12. Papazov, Y. Social Engineering, North Atlantic Treaty Organization; Science and Technology Organization:New York, NY, USA, 2016
13. O. O. Olagunju Adebayo, "An Analysis of the Impact of Mergers and Acquisitions on Commercial Banks Performance in Nigeria," ResearchGate, vol. 1, p. 1, 2012.
14. S. Ogunlere, "Impact of Cyber Crime on Nigeria Economy," ResearchGate, vol. 2, p. 12, 2013. "Social engineering fraud: questions and answers", Technical report, Interpol, December 2015.
15. https://www.thisdaylive.com/index.php/2016/11/02/preventing-social-engineering-attacks/
16. SANS Institute. Glossary of Security Terms; SANS: Boston, MA, USA, 2016. 15. Mitnick, D.S.W. The Art of Deception: Controlling the Human Element of Security; Wiley: Hoboken, NJ, US
17. Software Engineering Institute. Unintentional Insider Threats: Social Engineering; IEEE Security and Privacy Workshops: San Jose, CA, USA, 2014.