Cybercrime and Underground Attack Technologies: Perspectives from the Nigerian Banking Sector

[1]Alade, O.M., [2]Amusan, E.A.,[3] Adedeji, O.T. & [4]Adebayo, S.B.
Department of Cyber Security Science, Ladoke Akintola University of Technology, Ogbomosho, Nigeria
Department of Cyber Security Science Department, Ladoke Akintola University of Tech, Ogbomosho, Nigeria
Department of Information System Department, Ladoke Akintola University of Tech, Ogbomosho, Nigeria
Department of Computer Science Department, Ladoke Akintola University of Tech, Ogbomosho, Nigeria
Corresponding Authors' E-mails: [1]oalade75@lautech.edu.ng; [2]eaadewusi@lautech.edu.ng;
[3]otadedeji@lautech.edu.ng; [4]adebayo9424@gmail.com
Phone: [1]+2348161778639; [2]+2348038453840; [3]+2348132187577; [4]+2348063306593

ABSTRACT

Banks all over the world are taking advantage and opportunities brought about by e-banking which happened as a result of Internet. As the security level in this sector becomes stronger, the strength and tactics of these fraudsters also increases. Various lucrative attacks have been launched and unfortunately, many have succeeded. This paper addressed different types of cybercrimes in banking sector, factors contributing to cybercrime, tools used by cybercriminals, effects of cybercrime on Nigeria banking, cyber security technology for preventing cybercrimes and duties of individual and organizations on protecting our banks from cybercrime.

Keywords: Cybercrime, Banking Sector, Internet, Cyber security.

Proceedings Reference Format
Alade, O.M., Amusan, E.A., Adedeji, O.T. & Adebayo, S.B. (2021): Cybercrime and Underground Attack Technologies: Perspectives from the Nigerian Banking Sector. Proceedings of the 27th iSTEAMS Multidisciplinary Innovations & Technology Transfer (MINTT) Conference. Academic City University College, Accra, Ghana. June, 2021. Pp 49-54 www.isteams.net/ghana2021. DOI - https://doi.org/10.22624/AIMS/iSTEAMS-2021/V27P6

1. INTRODUCTION

The drive of emerging technology has brought a substantial changes to banking industry which makes it easier to render easy banking services to their customers. Banking sector in most part of the world was simple and reliable until mid-1990s, but since the advent of technology, the banking sector saw a paradigm shift in the phenomenon [4]. The advancement in ICT is accomplished by new threat and crimes known as cybercrimes. Cybercrime is any illegitimate activity and other illicit activities (committed against individuals or groups of individuals) that involve the use of telecommunications networks, in which computers or computer networks are instrument. The cyber underground economy (or cyber underground market) is a group of virtual marketplaces where cyber criminals buy, sell, and trade goods and services which thrive even in the perplexing global economic situations. The structure in which these transactions take place is now very refined, and includes job tasks such as cashiers who can transfer monies from stolen accounts into true currency.

2. LITERATURE REVIEW

Reference [4] discussed the problem of cybercrime in the banking sector within the Indian context and its impact on the bank's finances. It assesses the cybercrime scenario, examine the different types of cybercrime which plague the banking sector and the motives of the cyber criminals behind such acts. Reference [1] studied the cybercrime fundamentals, computer systems as a tools, content-related offences and cyberspace anonymity including privacy, security and crime control. In [5] technical aspects of various types of cybercrimes concerning the banking and financial sector and their related impacts was examined. It identified the threat vectors supporting these cybercrimes and develop measures to aid in the combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security. Reference [3] discussed how cybercrime affects the nation and the awareness and preventive measures by which one can overcome the threat.

In [2] an updated survey of cyber security was provided. Survey of security of recent prominent researches was conducted and categorize the recent incidents in context to various fundamental principles of cyber security. A new taxonomy of cybercrime which can cover all types of cyber-attacks was proposed. Various cyber-attacks as per the updated cybercrime taxonomy to identify the challenges in the field of cyber security was analyzed and highlight various research directions as future work. Reference [6] propose a new approach that emphasized on the prominent cybercrimes carried out in some major areas in Nigeria, precisely within secondary school students and presents a study of cybercrimes in these institutions within kebbi State and sokoto state. Also a new approach to Cybercrime prevention in order to efficiently combat cyber related crimes in Nigeria was presented.

This paper addressed different types of cybercrimes in banking sector, factors contributing to cybercrime, tools used by cybercriminals, effects of cybercrime on Nigeria banking, cyber security technology for preventing cybercrimes and duties of individuals and organization on safeguarding our banks from cybercrime.

3.. CYBERCRIMES IN THE BANKING SECTOR

In general, cybercriminals execute deceitful activities with the vital goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without legal approval. However, in some rare cases in Nigeria, the intention of cyber-criminals is to cause damage to the reputation of the bank by denying service to users and sabotaging data in computer networks of organizations [4]

3.1 Types of Cybercrime in Banking Sector

Bank Verification Number (BVN) Scams

The BVN is a biometric identification system which entails an 11-digit number that serve as a universal ID across all the banks in Nigeria. It was introduced to tie various accounts to the owner thereby ensuring that fake activities are reduced. It was revealed that wrong and illicit text messages and phone calls were sent to different users requesting for personal information such as their account details.

Phishing

Phishing can be defined as stealing of an identity. It includes stealing personal information from innocent users, legal businesses and financial institutions. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. In these operations, a spammer will send out e-mails that seem to come from a

bank in which people will willingly reveal financial information. These e-mails comprise a link to a website that again looks official, but only serves as a front to gather the required data like name, debit card number, and PIN.

Theft of Bank Cards

The theft of bank cards has advanced from the physical theft of the card to the theft of the numbers. Bank card hackers do not need to be in the same country to steal other people's identities. Fraudsters make use of secreted cameras to record ATM card pins and numbers in distinctive places where POS are being used or at the ATM center. Different applications can be used to retrieve this information such as key loggers at cybercafés or cloned websites.

Banking Fraud

Hackers target the vulnerabilities in the security of different bank systems and relocate money from numerous accounts to theirs. Most cyber-criminals transfer minor amounts like fifty kobo which are sometimes unnoticed by the user without making any enquiry. Doing this for above a billon accounts enriches the fraudsters.

Denial of Service

This attack is characterized by a clear effort by attackers to prevent genuine users of a service from using that service by "flooding" a network to disallow genuine network traffic, disturb connections between two machines to prohibit access to a service or prevent a particular individual from accessing a service.

ATM Skimming and Point of Sale Crimes

It is a method of conceding the ATM machine or POS systems by installing a skimming device on the machine keypad to look like a genuine keypad or a device made to be attached to the card reader to look like a part of the machine. Moreover, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers make the ATM machine to collect card numbers and personal identification number (PIN) codes that are later replicated to carry out fraudulent transactions.

3.2 Factors Contributing to Cybercrime in Banking Sector

a) Lack of fast and adequate fraud detection tools: Inadequate fraud detection tools to be installed in our various banks are major factor contributing to cybercrime in our banking sector. Without fraud detection tool it might be difficult to curb cybercrime in our banks.
b) Inadequate staff training and education in security practices: As the technology keep improving so also there is need to train staffs regularly and educate them on the use of new technology. Once staff were not adequately taught on security practices and procedures to follow, it will be difficult for them to know new tricks hackers are using to defraud their customers.
c) Absence of potential cybercrime risk assessment tools: A sector with no assessment tools is liable to be attacked easily. Most banks have little or no potential risk assessment tools which has really affect the banks in a negative way and such banks are prone to be attacked.
d) Poor security cultures: There is poor security cultures among users of mobile phones and gadgets used for on-line banking. This has greatly cause a lot of havoc to their properties and funds. Unprotected information like PIN, ATM cards, passwords gives cybercriminals to easily access their bank account and do away with their money.

3.3 Tools cyber-criminals use to execute cyber-crime

Exploit
An exploit is a piece of software or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unplanned or unexpected behavior to occur on computer software, hardware or something electronic. This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.

Vulnerability Scanner
A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from misconfigurations or flawed programming within a network-based asset such as a firewall, web server, application server, etc.

Password Cracker
A password cracker is software that recovers secret passwords from data that has been stored or transmitted by a computer system. Password cracking is the process of recovering passwords from data that have been stored or transmitted by a computer system.

Network Sniffer
Sniffing involves inspecting, capturing, decoding and interpreting the information inside a network packet that flows on a TCPIP network. The reason behind this is to steal information, which is usually in the form of user identity, passwords, network details and credit card numbers. It is a program or device that monitors data travelling over a network. Sniffers can be used both for valid network management functions and for robbery of information off a network.

Effects of cybercrime on Nigeria banking sector
(i) Loss of revenue generated by banks.
(ii) Disruptions of international financial markets
(iii) Loss of consumer confidence and trust
(iv) Insecurity of both life and properties

4. CYBERCRIME CONTROL SECURITY TOOLS

As a result of the notable development of recent electronic technologies and innovations associated with security, there is need to address the up-to-date technologies and procedures and the means to be taken to protect the information systems in the banking, financial and economic institutions.

Firewalls: A firewall is a system designed to prevent unapproved entrance to or from a private network. Banks implement a firewall in any hardware or software form, or a mixture of both. Firewalls avoid unauthorized internet users from gain access to private networks connected to the internet, especially intranets. All messages incoming or exit the intranet pass through the firewall, which scrutinizes each message and blocks those that do not meet the identified security criteria.

Intrusion Prevention Systems
An Intrusion Prevention System (IPS) is a network security/threat prevention technology that inspects network traffic flows to recognize and avert vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.

Anti-virus
Antivirus software also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Antivirus software was initially developed to detect and remove computer viruses, hence the name. With the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect users from computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy) and online banking attacks.

Data Loss Prevention Software
Data loss prevention software identifies potential data breaches and prevents them by monitoring, detecting and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage). Data loss incidents turn into data leak incidents in a circumstances where media containing sensitive information is lost and consequently acquired by an illegal party.

Encryption and Decryption Approach
Utilization of Secure Attachments layer can be used in e-management of an account. This gives encryption connection of information between a web server and a web program. The connection ensures that the information stays secret and secured.

5. PROTECTION OF THE BANKING SECTOR

Certain responsibilities must be carried out by individuals and organization to protect their banks from cybercrime and underground technology. Professionals and dedicated security teams should be employed to take a proactive stance when it comes to cyber security and privacy. A continuous cybercrime risk assessments must be carried out by banks to assess, identify and improve their present security measures by observing the organization's policies from an attacker's viewpoint and thus enable enhanced security, operations, organizational management. There should be an introduction of cyber awareness at a fundamental level in educational institutions with specialized security courses at graduate level to provide hands-on training on the latest attack methodologies and mitigation techniques using concepts like virtual cyber laboratory. From organization point of view, there should be comprehensive threat intelligence technology to foster, organized and analyzed threat information about current attacks. Bank employees must undergo periodic training.

Education to customers is also important. Customers must be mindful about the rules and regulations of e-managing of an account. Customers must be mindful about different bank cheats and be educated about security measures so that they don't fall prey as casualties of digital wrongdoing.

6. CONCLUSION

This paper examine the cybercrime and underground technology in Nigerian banking sector. However, the specific objectives were to examine types of cybercrime in banking sector, factors contributing to cybercrimes in Nigerian banking sector, the tools used by cybercriminals to perpetrate their criminal act in Nigerian banking sector, examine the effects of cybercrime on the banking sector and cyber-security technologies available on prevention of Cybercrimes in Nigerian banking sector. Duties of individual and organizations on how to protect our banks from cybercrime were also listed.

REFERENCE

[1] Chawki, M. Darwish, Khan and Tyagi (2015): Cybercrime, Digital Forensics and Jurisdiction. New York: Springer International Publishing.

[2] Harmandeep Singh Brar and Gulshan Kumar (2018): Cybercrimes: A proposed taxonomy and challenges. Journal of Computer Networks and Communications 1-11.

[3] Monalisa Hati (2016): Cybercrime: A threat to the nation and it's Awareness. International Journal of Advanced research in Computer and Communication Engineering. 5(7):690-692.

[4] Raghavan A. R. and Parthiban Latha (2014): The effect of cybercrime on Bank's Finances, International Journal of Current Research and Academic Review. 2(2):173-178

[5] Seema Goel (2016): Cyber-Crime: A growing Threat to Indian Banking Sector. 3rd International Conference on Recent innovations in Science, Technology, Management and Environment, India. 13-20.

[6] Wisdom D.D, Ajayi E.A., Hamza M.K. and Odewale O.O. (2019): Cybercrime: A threat to a moral society. 2nd International Conference on education and development. 364-375.