EasyChair Preprint

№ 3595

The problems of Cybercrime in Banking Industry: Impact and Challenges

Abdullahi Idris and Ismail Mato

June 11, 2020

THE PROBLEMS OF CYBERCRIME IN BANKING INDUSTRY:

IMPACT AND CHALLENGES

By

ABDULLAHI IDRIS[1]

College of Science and Technology,

Department of Computer Science,

Jigawa State Polytechnic, Dutse, Nigeria

abdul_idrith@yahoo.com, sankararng@gmail.com

08066695424

ISMA'IL MATO[2]

College of Science and Technology,

Department of Computer Science,

Jigawa State Polytechnic, Dutse, Nigeria

ismailmato11@gmail.com

08069770886

BEING A PAPER SUBMITTED FOR PRESENTATION AT 2020 INTERNATIONAL CONFERENCE ORGANISED BY NIGERIA COMPUTER SOCIETY

EATI'2020

Abstract

Whatever is good has potential of being bad or evil when properly exploited by relevant agents. It only remains good when its bad potentials have not been identified and tapped. This saying is true when the usage of the web and its associated packages come into the spectacle. As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cybercrimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cybercrimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. This work seeks to define the concept of cyber-crime, identify causes of cyber-crime, how it can be eradicated, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

Keywords: Cybercrime, security, phishing, hacking, ATM crimes, Vishing cyber, Malware

1.0 Introduction

The evolution of technology has increased the dependency of humans on it in all spheres of life. In addition to the opportunities, benefits, accuracy provided by these inventions, it however increased the probability of getting trapped in cybercrimes. Undoubtedly, cybercrimes are frequent these days and financial sectors are majorly targeted by hackers or criminals. Most of the organizations rely on the digital networks for their business operations which increases the risk of becoming a victim of cybercrime. Cybercrime also known as computer crime, is the use of a computer as an instrument to further illegal ends on internet through which hackers invade into financial or private accounts of users with wrong intention without their authorization. Banks in order to enhance their customer base introduced many platforms through which transactions could be done without much effort. Computers and network are used for cybercrimes which include credit card frauds, phishing, spams, blackmail, forgery and many other frauds.

New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: There are bundle of numbers and identifiers in multiple computer databases owned by Banks. Cybercrime highlights the centrality of networked computers in lives, as well as the fragility of such seemingly solid facts as individual identity.

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Cybercrime Convention was signed by 30 states. Additional protocols, covering terrorist activities and racist and xenophobic cybercrimes were proposed in 2002. In addition, various national laws, such as the USA PATRIOT Act of 2001, have expanded law enforcement's power to monitor and protect computer networks.

Banks are targeting more by criminals than any other sources, it has been always seen that cybercrimes are directly proportional to less security measures taken by people on the computers and revealing of the passwords, PINs, card number of credit and debit cards. Criminals are dependent upon these numbers to commit a crime. These numbers actually represent a customer's authorization to operate an account. Without these it is difficult to penetrate the security.

The significance of the study is make aware the users of online banking and make some recommendations to improve the security on the electronic system and how it can be minimize or eradicated by adopting some measures.

2.0 Cybercrime Challenges

Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories:

1. Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, malware etc.
2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams, ATM crimes and information warfare.

2.1 Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cybercrime (Hassan, 2012)

(a). Unemployment is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.

(b). Quest for Wealth is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.

(c). Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

(d). Incompetent security on personal computers. Some personal computers do not have proper or competent security controls, it is prone to criminal activities hence the information on it can be stolen.

.

2.2 Various Cybercrimes in Nigeria

Over the past decade, the internet has experienced an explosive growth with the number of hosts connected to the internet increasing daily at an exponential rate. As the internet grows to become more accessible and more services become reliant on it for their daily operation, so does the threat landscape. In Nigeria, cybercrime has become one of the main avenues for pilfering money and business espionage. According to Check Point, a global network cyber security vendor, as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa (Ewepu, 2016). Nigerians are known both home and abroad to be rampant perpetuators of cybercrimes. The number of Nigerians caught for duplicitous activities carried by broadcasting stations are much more in comparison to other citizens of different countries. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, these sectors such as the banking, ecommerce and educational sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor. Therefore, in this section, prominent specific ways in which cybercrimes are mostly carried out in Nigeria are discussed.

2.3 Cybercrimes in the Banking Sector

The life wire of the banking sector is the internet. Currently, banks all over the world are taking advantage and incorporating opportunities brought about by e-banking which is believed to have

started in the early 1980's (Shandilya, 2011). As the security level in this sector becomes stronger, the strength and tactics of these fraudsters increases also. Various lucrative attacks have been launched and unfortunately, many have succeeded. In general, cybercriminals execute fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without rightful authorization. However, in some rare cases in Nigeria, the intention of cybercriminals is to cause damage to the reputation of the bank by denying service to users (Parthiban, 2014) and sabotaging data in computer networks of organizations.

2.3.1 Bank Verification Number (BVN) Scams: The BVN is a biometric identification system which consists of an 11-digit number that acts as a universal ID across all the banks in Nigeria. BVN was implemented in 2015 by the Central Bank of Nigeria. It was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minimized. For fraudsters, opportunities to extort money and to carry out other fraudulent activities arose from the implementation of the BVN. It was detected that fake and unauthorized text messages and phone calls were sent to various users demanding for personal information such as their account details. In addition, phishing sites were created to acquire such information for insalubrious activities on the bank account. **Phishing**: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorized businesses and financial institutions that are victimized (Wada). Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. In this jet age of technology, hoi
polloi subscribe to a plethora of sites using their email addresses and are therefore expecting to receive mails of updates of their membership or subscription. So it seems natural when users get regular mails from such organizations. Fraudster have devised a means to mimic authorized organizations and retrieve confidential information from clients. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. An instance of such mail is shown in the figure below showcasing a fraudster trying to build the trust of a client in order to convince them to give up personal banking information. In Nigeria, phishing mails are mostly carried out on bank customers. Fig 1. Phishing e-mail message **Theft of Bank Cards**: The theft of bank cards has evolved from the physical theft of the card to simply the theft of the numbers. Today, bank card hackers do not need to be in the same country to steal other people's identities. Fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS, or at the ATM. According to the Federal Bureau of Investigation (FBI), a method known as ATM skimming can be used and it involves placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine (FBI, 2011). Also, another cybercrime carried out via this means in Nigeria includes internet order fraud. Internet order frauds involves fraudster inputting stolen cards numbers on online commercial sites to order goods. Credit card numbers or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. Different applications can be used to retrieve this information such as key loggers at cybercafés or cloned websites.

2.3.2 Cyber-theft / Banking Fraud: Hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs. Most cybercriminals

transfer bantam amounts like 5 naira which are sometimes overlooked by the user without questions raised by the users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most fraudsters.

3.0 Impact of cybercrime

The Nigerian economy, including the enormous amount of banking industry, is greatly threatened by the rapid increase of e-crime, to study the impact of cybercrime two methods are used to identify how much strong the system of cyber attackers are: Qualitative analysis as well as content analysis are used. In qualitative analysis, 200 respondents were interviewed from different countries including Canada, Nigeria, Ghana, India and Malaysia, asking the awareness about cyber threats in banking industry, some are victims while some are aware and conscious.

The most common fraud that was found in Canada is Vishing, Vishing is an offence that one can commit through voice calls. In Vishing criminals pretend to be calling from an official source of their country and threatens the consumers in order to get access to their personal information, or account details. Most vishing attempts try to convince victims to give up their PIN, Card number, SIN number, banking accounts passwords and their personal details.

3.1 Qualitative Analysis Summary

Figure 1.0

S/N.	COUNTRY	METHOD	AGE BRACKET	COMMON FRAUD	SUMMARY OF YEARS
1.	Canada	Interview	20-25	Vishing	2017
2.	Nigeria	Interview	25-30	ATM Crimes	2019
3.	Ghana	Interview	30-35	Phishing	2018
4.	India	Interview	35-40	Malware	2017
5.	China	Interview	40-45	Hacking	2017

The above table represent the summary of qualitative analysis base on age bracket conducted by the respondent through questionnaire by five countries and finally retrieved the common fraud type conducted in terms of age bracket.

3.2 Content Analysis

Consumer loss through cybercrime worldwide in 2017, by victim country (in billion U.S. dollars). From the figure 1.0 it can easily measure that cybercrimes affected major world in 2017. China has experienced a loss of 66.3 billion dollars in 2017 which is the highest. Globally, the average cybercrime victim lost 142 U.S. dollars (The Statistics Portal, 2017). In the analysis, it was found out that cybercrime is a big concern all over the world. All types of crimes like Vishing, ATM Crimes, Phishing, Malware and Hacking is prevalent in most countries. Banks can prevent these crimes to some extent, recurrence of these incidents will affect the digital economy. Negligence by customers and IT sector is the another reason for cybercrime. Other institutions can also make people aware of the prevailing scams, for examples, government organizations, schools and colleges.

4.0 CONCLUSION

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to break even. Several prominent cybercrimes and causes have been discussed in this paper. The study conducted in the five selected countries as regards to the cybercrimes in banking industry, impact and challenges in cybercrimes shows that majority of the crimes conducted are carried out by the youths in our society majorly through phishing, Vishing, Malware, ATM crimes and hacking. have been proposed to prevent future occurrence of this crime, however much can still be done by government and individuals to reduce it. It is recommended that government should make the welfare and wellbeing of the citizens of paramount importance so as to lessen the burden of individuals by providing good paying jobs and other basic amenities. This will in no little way make life comfortable for people hence reduce their participation in criminal activities for survival. It is only after this is done that any bill or law against cybercrime can really take effect. Individuals are also enjoined to be smart and adhere to the preventive measures listed above in order not to fall victims. Moreover, since youths are the most involved in this crime, there is need for orientation, educating and empowering for the country to have a greater future. Banks should work in cooperation with other banks across the world to prevent cybercrimes.

REFERENCES

1. Hassan, A. B. Lass F. D. and Makinde J. (2012) *Cybercrime in Nigeria:Causes, Effects and the Way Out,* ARPN Journal of Science and Technology, vol. VOL. 2(7), 626 – 631.

2. Lakshmi P. and Ishwarya M. (2015), *Cyber Crime: Prevention &Detection*," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).

3. Maitanmi, O. Ogunlere, S. andAyinde S. (2013), *Impact of Cyber Crimes on Nigerian Economy,*

4.MichaelA.,Boniface., A. and Olumide, A. (2014) *Mitigating Cybercrime and Online Social Networks Threats in Nigeria*, Proceedings of the World Congress on Engineering and Computer Science, 22–24.

5. Ndible N., (2016*) Practical Application of Cyber Crime* Issues, 36-57

6. Shandilya A. (2011) *Online Banking: Security Issues for Online payment*, 39-73

7. Okeshola F.B. and Adeta A.K, (2013) *The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria* American International Journal of Contemporary Research, vol. 3(9),98-114.

8. Parthiban L. and Raghavan A. R. (2014), *The effect of cybercrime on a Bank's finances,* International journal of Current Research and Academic.

9. Wada F. and Odulaja G. O. (2014), "Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation.

10. Ewepu G, (2016) *Nigeria loses N127bn annually to cyber-crime* — NSA