Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, August 2017, vol. 22, no. 2

INTERNET BANKING: IDENTITY THEFT AND SOLUTIONS - THE NIGERIAN PERSPECTIVE

DEBORAH UZOAMAKA EBEM

Department of Computer Science, University of Nigeria, Nsukka, Nigeria

Tel: +2348052810722, +238185171069;

Email: **deborah.ebem@unn.edu.ng**

JOSEPH CHINONYE ONYEAGBA

Department of Computer Science, University of Nigeria, Nsukka, Nigeria

GERALDINE EGONDU UGWUONAH

Department of Marketing, University of Nigeria, Nsukka, Nigeria

Abstract

An eclectic observation of the Nigerian financial landscape reveals that identity theft and financial related crimes are on the rise. Having engaged the use of Information and Communication Technology (ICT) as a platform for effective and efficient means of conducting financial transactions, the financial sector is also battling with the accompanying risks. In this research work, we want to know if there are relationships between lack of proper information dissemination, computer literacy and high rates of identity theft/financial crimes in Nigeria. Questionnaires were distributed to randomly select internet-banking users, interviews were conducted and from our findings, we reached the consensus that lack of proper knowledge and means/forms of identifying cybercrime related emails, texts and phone calls are responsible for the high rate of identity theft in Nigeria. Granted that banks will never ask for financial information via emails, cybercriminals are exploiting other social engineering

techniques to perpetrate identity theft. We also identified loopholes in the typical Nigerian bank customer care department sequence of communication which cybercriminals tend to exploit. Hence, we highlighted means of identifying possible email related phishing scams. Finally, effective prevention techniques were discussed.

Keywords: **Cybercrime; Identity Theft; Internet Banking; Phishing; Prevention**

INTRODUCTION

Following the boost of the ICT sector in Nigeria in year 2000 and the electronic-banking revolution which started in 2003, total awareness and use of electronic means of payment has been on the increase and currently stands at over 20 Trillion Naira [1,2]. Some of the reasons adduced for this increase in the volume of internet banking as pointed out [3] includes cost savings, less branch networks and downsizing of the number of service staff- thereby paving way for self-service channels. Apparently, the customers of these banks enjoy self-service, freedom from time and space constrains and reduced stress of queuing in banking halls [4].

Unfortunately, despite the giant strides and achievements of internet banking, the Nigerian financial sector is currently battling with the twin evils of identity theft and financial frauds, just like other advanced economies of the world. A report [5] in 2014 estimated that about 0.8% of Nigeria's Gross Domestic Product (GDP) is lost to cybercrime and [6] estimated this to be equivalent to the worth of the nations' cement sector. With major advances in ICT and its related technologies such as Internet Protocol (IP) tracking, Euro pay, MasterCard and Visa (EMV), Address Verification System (AVS), advanced economies have made some tremendous progress in trying to keep most cyber criminals away from their cyber space. As expected, financial crime perpetrators have turned to softer targets to carry out their illegal activities.

With over 97 Million internet users on daily basis [7], 45.3% of whom suffered internet related attacks in the third quarter of 2015 [8]; the Nigerian Cyberspace provides a lucrative hub for cybercriminals. But what are the natures of these cybercrimes and how do cybercriminals acquire the necessary information needed to execute these heinous crimes? These are the questions this paper seeks to address.

RESEARCH AND METHODOLOGY

A detailed research in Monica [9] which was presented in 2012 was firm in his opinion that “awareness is the best defense”. In a candid bid to answer the question posed above with regards to how cybercriminals obtain the necessary information

needed to execute ID theft related crimes, we employed a general -interview-guide approach to extract first-hand information from internet banking users via short interviews in some selected locations. The pool of respondents cuts across every strata of the society, taking into considerations factors such as age, sex, religion and educational background.

A three-scale response pattern questionnaire was designed, comprising of the answers
1. No
2. I don't know and
3. Yes.

A total of 2500 questionnaires were distributed and 2358 were collated after the exercise. The collated data were analyzed and the result is shown in the Table 1.

Table 1: Showing the result of analyzed questionnaire.

S/N	Question	Yes (%)	I Do Not Know (%)	No (%)
1.	Do you have an active internet banking account?	57	11	32
2.	Have you ever heard of Identity Theft?	30	13	57
3.	Have you ever received an email, SMS or phone call from someone requesting for your banking details such as ATM	82	8	10
4.	Have you ever disclosed your banking details to someone who claims he/she is calling to help you rectify your Bank	69	19	12
5.	Has your bank ever taught you how to avoid identity theft?	10	10	80
6.	Do you know your bank's customer care phone number?	7	4	89
7.	Do you have access to the Internet and can you use a computer or smart phone effectively?	80	09	11
8.	Have you ever lost money to internet fraudsters or "yahoo yahoo boys"	70	09	21

Hence, from the result of the collated questionnaire, it is glaringly obvious that ignorance is a major factor which contributes to identity theft.

The Concept of Identity Theft

Identity theft is a term used to refer to fraud that involves pretending to be someone

else in order to steal money or get other benefits [10]. In Nigeria considering the sophistication and technical expertise invested in identity theft, it is safe to conclude that 90% of these attacks are financially motivated [9,11]. Opined that cybercrimes (which includes identity theft) are economic crimes committed using the computer and the internet. She was of the opinion that cybercrimes include distributing viruses, illegally downloading files, phishing, pharming and stealing personal information like bank details.

Identity Theft and the Prevailing Techniques

One of the most common identity theft techniques in Nigeria is social engineering. The social engineering attacks aim at either coercing or tricking an individual into disclosing his personal information such as bank account details, emails details and so on. Under social engineering, the three prevailing identity theft techniques are:

(i) email based phishing scam,
(ii) Short Message Service (SMS) scam and
(iii) Phone calls related scam.

In the following sections of this work, we will explain the steps, techniques and some practical ways of identifying these most prevalent identity theft techniques in Nigeria with the aim of helping unsuspecting users to identify and avoid them.

Phishing

The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords by impersonating a trust worthy person or business (e.g., financial institutions) in an apparently official electronic communication [12]. "Phishing" is simply an alteration of the word "Fishing". Here, the perpetrator is the fisherman, the email the bait and the targeted victim being the fish.

With the proliferation of web development platforms and its associated technologies, cloning an official website (or webpage) is easier than ever. The basic tools which a cybercriminal needs to setup an email based phishing scam are:
1. A hosting platform - (Cpanel or Shell) - available online for sale on the following websites
Spammer.ro
bigsh0p.us
spam-lab.su
2. A cloned web page(s) - (Also known as Scam Page(s)) - available online for sale on the following sites
ish0p.cc
Spammer.ro
3. An automated email mass sender - available online for sale on the following sites

mailworld.info
bigsh0p.us
4. A list of email addresses (also known as "leads") - available online for sale on the following sites
mailworld.info
bigsh0p.us
spam-lab.su
5. An electronic wallet for payment (e.g., bitcoin, perfect money etc.) available online.

Since anyone with basic knowledge of web development and hosting can setup an email based phishing scam and the tools are readily available online, the major task for the average user of internet banking is identifying the real webpage(s) and differentiating it from the scam pages.

Here, we will discuss some of the techniques/ways of identifying the real pages to avoid falling victim to email based phishing scam.

Steps to Identifying an Email Based Phishing Scam

Figure 1: A typical example of an email based phishing scam.

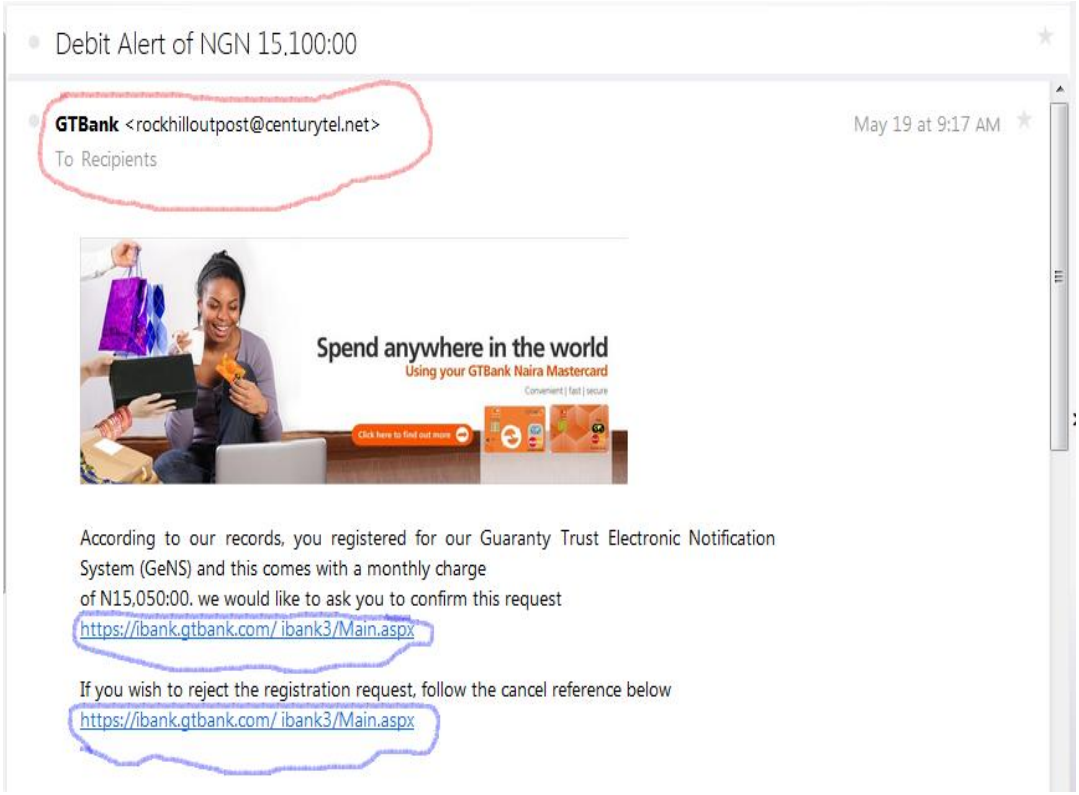
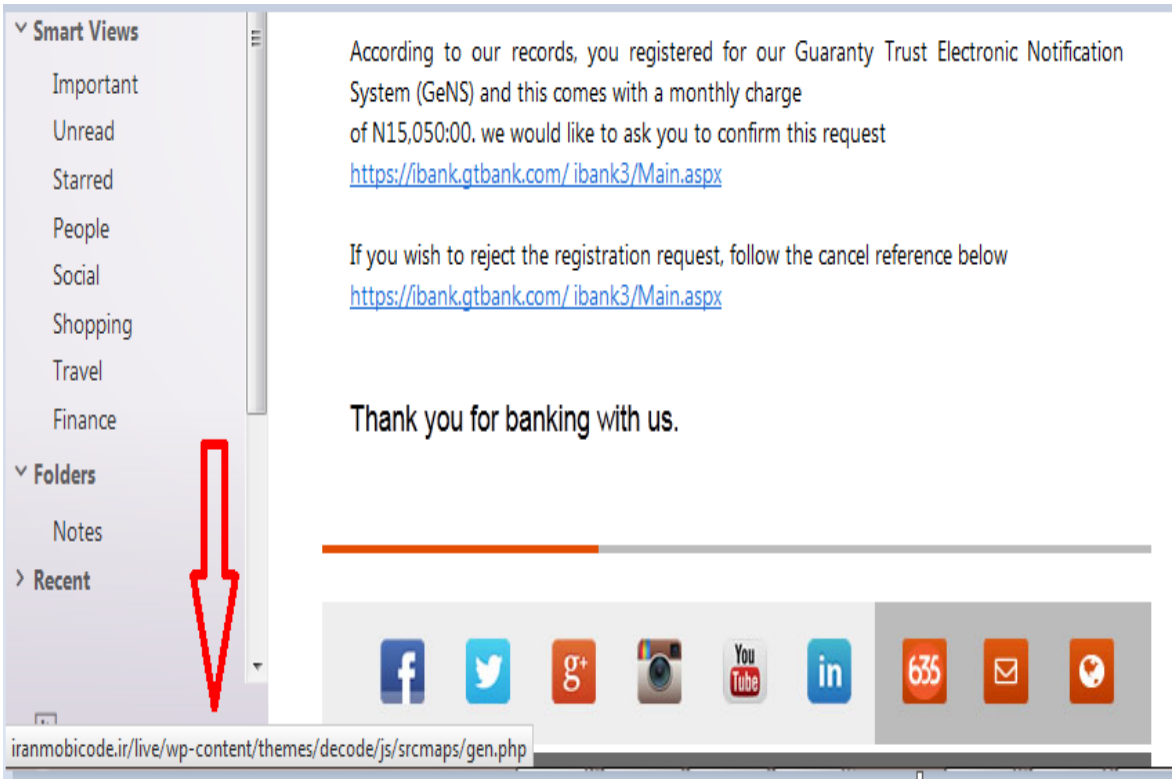


Figure 1, Internet banking users must be on the lookout for the following signs:
Multiple Recipients: One of the easiest ways of identifying an email based phishing

scam is the multiple recipients. Using automated tools such as PHP mailer or Advanced Mass Sender (AMS), it is fairly easy for cybercriminal to send scam emails to one thousand people within five minutes. From Figure 1, the area circled in red show the senders' address as well as the addresses of the recipients. Notice that the originating address is rockhilloutpost@centurytel.net, the domain name "centurytel.net" does not belong to GT Bank, and hence, the email looks suspicious. Also, notice that there are other “recipients" of this same email. However, there are "Targeted" scam emails where the recipient is the sole target and He/ She might be addressed by name and some account details (such as location, date of birth, account number and so on provided, it's all aimed at sounding more convincing and making the recipient believe the email was from the impersonated financial institution. The following steps below can help determine the authenticity of such email.

Perform Link Preview: Hovering the cursor over the directed link/hyperlink will activate the link preview feature of the page. Simply place the cursor on the link and observe the URL displayed at the status bar of the computer. If the link in the email and the displayed link on the status bar are not the same, it is possible that the perpetrator(s) might have "masked" the hyperlink. In Figure 2, the red arrow shows the URL displayed when we performed link preview.

Figure 2: Link Previews showing a “masked” hyper link.



The current trend involves the use of smart phones and tablets to check emails. If by chance the device does not have the capabilities to carry out the instructions in step (2), we recommend the next step of detecting email based phishing scams as pointed out by Goetz [13] the URL inspection algorithm.

The URL Inspection Algorithm

This generic 3-steps algorithm is quite simple and can be handy for the non-computer expert in identifying fraud related phishing websites. Here are the steps:
1. Look at the URL of the page you have landed on after clicking on the link.
2. Skipping over the leading http:// or https:// character at the beginning of the URL and scanning from the left to right, stop at the first forward slash character "/" you come to.
Note: most phishing websites don't contain http:// or https:// in their URL.
3. Examine the characters IMMEDIATELY to the left of the forward slash character before the dot character "."; these characters must be the domain name of the legitimate bank or financial company.

We will buttress the above steps with examples as it relates to most Nigerian banks. Figures 3 and 4 shows the legitimate login page of two Nigerian banks.

Figure 3: GTBanks' login page and URL.

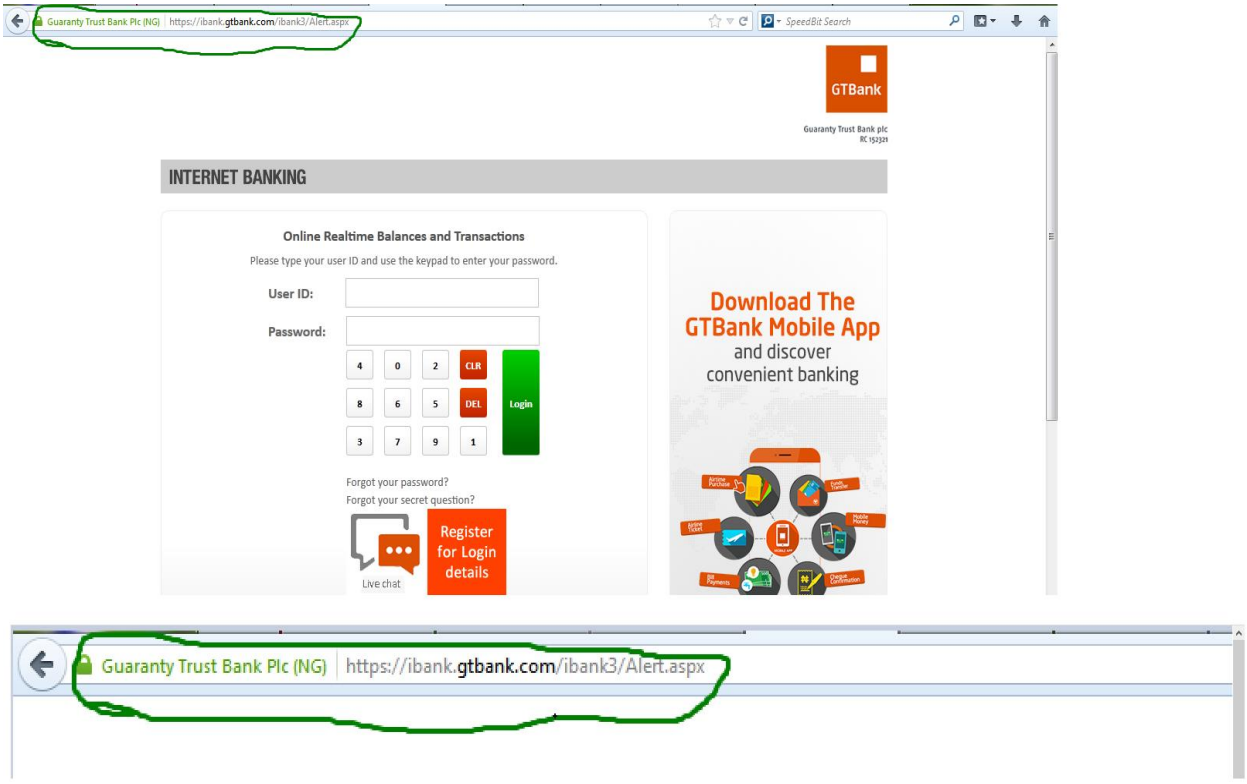


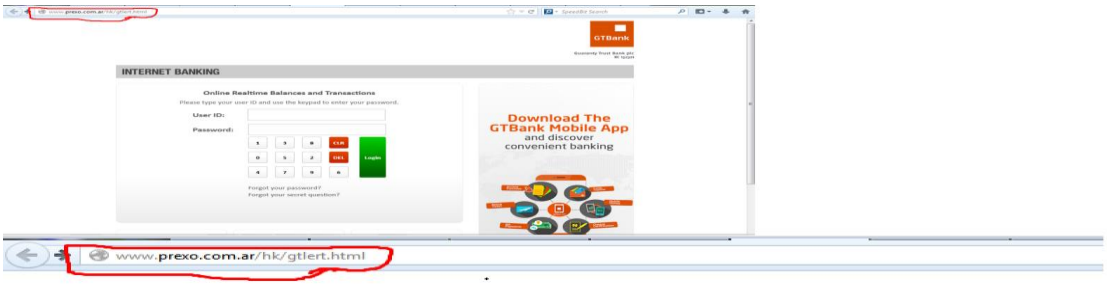
Figure 4: Sterling Banks' login page and URL.

Sterling Bank
The one - customer bank.

The Figures 3 and 4 shows a typical internet banking login page of Nigerian banks and their respective URLs. Applying the URL inspection techniques here, we can see that scanning from the left to right of the URL, the first characters IMMEDIATELY to the left of the first forward slash are "gtbank.com" and "sterlingbankng.com" which are the legitimate domain names of the two banks respectively.

Now, let's take a closer look at the fake GTbank login page in Figure 5 below.

Figure 5: FAKE GTBanks' login page and URL.



INTERNET BANKING

Inspecting the URL in Figure 5 above, it is important to note that certain features were missing. These include:
1. The Secure Sockets Layer (SSL) logo and its associated green colour. The SSL technology ensures that every data you send from your computer to the server remains private and integral, hence; reducing the possibility of someone high jacking your data. Nigerian banks have adopted the 128 bit SSL encryption security measures; hence, all their internet login pages must carry the SSL logo and the green colour.
2. The "http://" or "https://" characters are missing.
3. Applying the URL inspection technique, the domain name before the first forward slash character is "prexo.com.ar" instead of "gtbank.com".

It is important to note that cybercriminals can create a phishing website URL that might look like:
http://www.gtbank.com.8639127657.xyz.net/email/current/whp/gtalert.html

At first glance, the above URL might look genuine to unsuspecting victims. In fact, http://www.gtbank.com can be seen clearly at the beginning of the URL. But applying the URL inspection techniques, it can be clearly seen that the characters to the IMMEDIATE left of the FIRST forward slash character is xyz.net and not gtbank.com. Hence, it is safe to conclude that the website is a phishing site.

Scam Related Text Messages and Phone Calls

Following the introduction of Bank Verification Number (BVN) into the Nigerian financial sector on February 14, 2014, cybercriminals and identity theft perpetrators saw a lucrative avenue to continue their illegal activities. The BVN is a ten-digit number issued to a bank customer who has completed the biometric captures as stipulated by the Central Bank of Nigeria (CBN).

The BVN project was conceived and executed with the sole aim of enhancing security within the financial sector, as the existing security measures such as passwords and pin were failing. At the peak of the exercise when customers' bank accounts were frozen for failures to register and obtain the BVN within the stipulated timeframe, cybercriminals (who were impersonating legitimate bank staff started contacting bank customers, requesting for their bank details, promising to help them unlock their bank accounts. This resulted in loss of substantial amount of money after the account has been activated by the bank when the customer eventually registers and obtains the BVN.

Till date, there are still cases of cybercriminals who visit sites such as truecaller.com, 'harvest' phone numbers and the names of registered owners, send text messages to these phone numbers, addressing the owners by their first or last names while informing them that their BVN registration was incomplete. They will require them to send some financial information such as ATM pin, account number and so on to

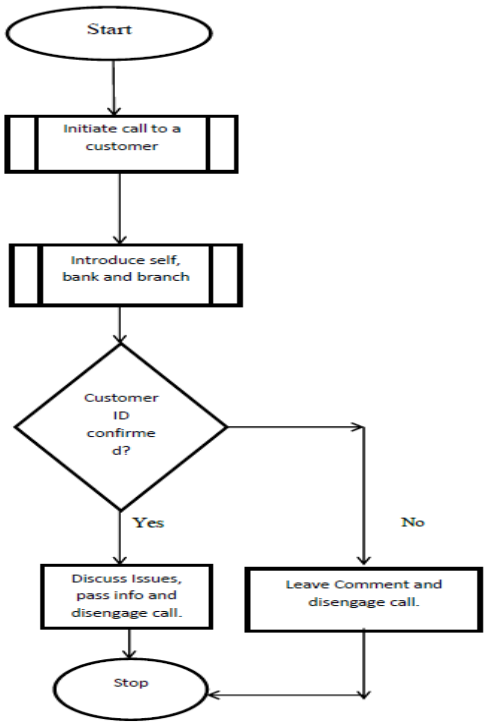
enable them rectify one issue or the other.

NIGERIAN BANKS, CUSTOMER CARE DEPARTMENTS AND IDENTITY THEFT - ISSUES ARISING

The customer care service departments of Nigerian banks are responsible for attending to customers' inquiries and for contacting the customers if there are issues such as identity theft and other related issues or discrepancies. A careful study of these communication channels reveals that banks reach their customers via emails, text messages and phone calls. Each bank has a dedicated customer service phone number which is centrally controlled from the headquarters of the banks. This leaves the bank's branches to the use of other phone numbers as the official means of contacting customers via phone calls from their respective branch offices. Although these branch offices phone lines are registered to the banks, there are no features which show that they belong to or are registered to these banks.

After a careful examination and the use of general-interview-guide approach to extract first-hand information from heads of customer care departments, the flow chart below shows the simple sequence of communication flow from the customer care representative of a bank branch to a customer (Figure 6).

Figure 6: Communication flow sequence from customer care unit to customer in Nigeria banks.



A careful examination of the steps in the flow chart above shows a room for impersonation/identity theft. This is apparent as a major population of customers sampled in the banking halls of different banks visited admitted to not knowing the customer care phone numbers of their respective banks where their account(s) is domiciled or that of any branch customer care department.

The implication of this is that identity theft perpetrators and cybercriminals can impersonate a bank official, call a bank customer and obtain valuable financial information. This act becomes easier if the cybercriminal has obtained any previous data on that customer. To sound more convincing, the cybercriminal might quote the customers' account number, account name, branch of domicile, account balance, last debited amount and so on.

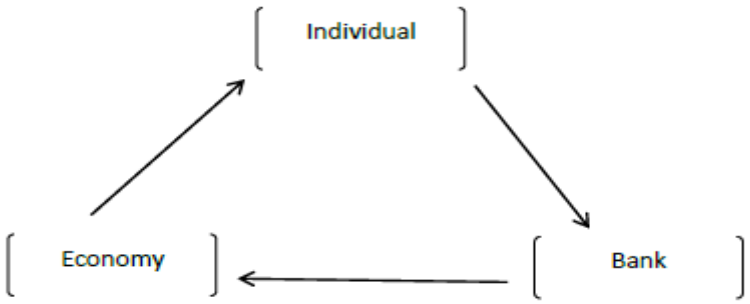
Of course, it is important to note that the information listed above are very easy to get, as most bank customers don't keep papers containing their banking details properly. Automated Teller Machines (ATM) receipts, POS receipts, partially used bank deposit slips and so on. All serves as 'mining field' to cybercriminals. Information 'harvested' from these social engineering processes can be used to initiate funds transfer from customers' internet banking accounts or they can as well be used to clone their ATM cards. This results in loss of millions of Naira yearly in Nigeria.

Preventing and Fighting Identity Theft

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes) [14].
The psychological and economic effects of identity theft are more pronounced on the victim. The effect cycle below shows that the harsh effects of identity theft starts and ends with the individual/victim.

Hence, the individual has a greater role to play in the prevention and management of this menace (Figure 7).

Figure 7: Identity theft effect cycle.



In the light of the foregoing, we believe that what can be done is preventing and controlling identity theft, since it is almost impossible to eliminate it; and it all starts with the individual, although the banks and government have their roles to play. The following measures if well employed can prevent identity theft, thereby reducing the financial loss that results from identity theft:

Vigilance

Research in Gercko [15] has shown that identity theft is not possible without the 'cooperation' of the victim. More often than not, legitimate account holders are the ones who give out their financial information by cheer carelessness, negligence or largely due to their inability to identify phishing scams (an exception are those whose computers were infected with malwares such as Zeus botnet and Trojan horses).

The steps discussed in this work can be very handy in detecting email based phishing scams. Applying the three steps carefully reduces the chances of falling for email based phishing scam by over 70%. With respect to text messages and phone calls, internet banking users and bank customers are advised to get the phone number(s) of the customer care departments of their respective banks. When a customer receives such suspicious text messages or calls, the best protective measure is to hang up and contact his/her bank for clarifications.

The Use of Antivirus and Anti-Phishing Software

In this information age, there is software that can detect and block phishing websites. Most antivirus software also has the anti-phishing components built into them. These software ranges from free versions to paid versions. Internet banking users are advised to install anti-phishing software on their computers and tablets and also ensure that they are updated regularly.

Awareness

The banks have a larger role to play in this perspective. Available statistics from our research reveals that over 70% of identity theft victims are individuals within the age bracket of 40-70 years who have very little knowledge of ICT. This population comprises of the market women, artisans, civil servants (both retired and active), commercial drivers and so on, who had very little formal education and can barely read or write.

Following the introduction of cashless policy in Nigeria on July 1st, 2014, a largely uneducated population of the country who hitherto, draws money over the counter in the banking halls were forced to adopt the use of ICT and its tools as a means of conducting transactions. By the virtue of being uneducated, a large percentage of them cannot read and understand the numerous warnings their banks display on the ATM and notice boards.

We hereby suggest a holistic grassroots awareness campaigns which includes visiting places such as churches, mosques, markets, motor parks and so on, where bank officials can sensitize people in their local dialects about the concept of identity theft, the implications and ways of avoiding it. Radio jingles, television adverts and periodic reminders via emails and text messages can also help the younger generations in combating identity theft. Banks are also advised to ensure that their customer service phone numbers are toll free. This will ensure easier access to the banks from their customers.

Provision of Economic and Social Infrastructures

Every year, the Nigerian tertiary institutions churn out over six hundred thousand graduates [16], 50% of whom are proficient in the use of ICT and the internet. The Nigerian labour market can barely absorb 20% of these graduates and the required economic and social infrastructures which are prominent to successful start-ups of Small and Medium scale Enterprises (SMEs) are virtually nonexistent. Hence, some of this army of unemployed youths turns to cybercrime as a means of making ends meet [17].

To reduce cybercrime and identity theft, the Federal Government of Nigeria needs to as a matter of urgency, fix the social and economic infrastructures of the country. As a failure to do so will attract more sophisticated cybercriminals to the Nigerian cyber space, thereby resulting in more financial loss and capital flight.

Enforcing and Strengthening Existing Laws

Cybercrimes are very lucrative and it can be difficult to wean a perpetrator off the crimes. The law enforcement agencies must be willing to wield the big stick of the law when perpetrators are apprehended. This will serve as a deterrent to intending cybercriminals. The law enforcement agencies and the judiciary must work in resonance to ensure proper and speedy investigation, trial and conviction of cybercriminals. Also, the legislative arms of government must strengthen the existing laws as well as make new laws to combat identity theft and other related cybercrimes.

CONCLUSION

Identity theft has become a problem to the Nigerian financial sector, resulting in the loss of millions of naira yearly. As the Federal Government of Nigeria continues to enforce the cashless policy, more people are embracing internet banking and e-commerce; there is an urgent need to curb the menace of identity theft.

In this research work, an attempt was made to discuss the concept of identity theft, the prevailing techniques employed by cybercriminals and ways of detecting social engineering based scams. Finally, we proffered measures for preventing and

combating these cybercrimes. We are of the opinion that the individual, banks and the government all have a role to play in combating identity theft, but it all starts with the individual internet banking user.

REFERENCES

1. Ayo CK, Adebiyi AA, Fatudimu IT, Ekong OU (2008) Framework for e-Commerce Implementation: Nigeria a Case Study. Journal of Internet Banking and Commerce.
2. 2014 e-payment fraud landscape in Nigeria - A summary and analysis of reported e-payment frauds: Pikkarainen T, Pikkarainen K, Karjaluoto H, Pahnila S (2004) Consumer acceptance of online banking: an extension of the technology acceptance model 14: 224-235. www.emeralinsight.con/researchregister
3. Aderonke AA, Ayo Charles K (2010) An Empirical Investigation of the Level of Users' Acceptance of E- Banking in Nigeria. Journal of Internet Banking and Commerce. http://www.arraydev.com/commerce/jibc/
4. (2014) Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
5. Abdul-Hakeem A. Targeted attacks: Protecting Critical National Infrastructure. http://cybersecurenigeria.org/wp-content/uploads/2015/11/CSEAN-Emerging-Cyber-Security-Threats-6-7April16-Abdulakeem-Ajijiola.pdf
6. Nigerian Communications Commission Internet Subscriber Data. http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=68&Itemid=70
7. Kaspersky Lab (2015) Survey, for Third quarter 2015 IT Threat Evolution report. http://bizwatchnigeria.ng/nigerias-cyber-malware-attacks-reach-45-3-in-q3-201
8. Arunachalam P. Economic Impact of Identity Theft in India: Lessons from Western Countries. http://www.ipedr.com/vol12/42-C106.pdf
9. Monica NA (2013) Challenges of using IT to Combat Economic Crime. Afr J of Comp and ICTs 6: 31-36.
10. Hedayati A (2014) An analysis of identity theft: Motives, Related frauds, Techniques and Prevention. Journal of law and conflict resolution. http://www.academicjournals.org/article/article1379859409_Hedayati.pdf
11. Jakobsson (2007) The Human Factor in Phishing. http://www.informatics.indiana.edu/markus/papers/aci.pdf
12. Gercke M (2007) Criminal Liability for Identity Theft and Phishing, CR 2005, 606; Paget, Identity Theft. McAfee White Paper http://www.mcafee.com/us/threat_center/white_paper.html

13. Goetz P. Algorithm for Detecting Phishing Websites. https://sites.cns.utexas.edu/oit-blog/blog/algorithm-detecting-phishing-websites
14. https://www.techopedia.com/definition/2387/cybercrime
15. Gercko M (2007) Internet-related identity theft. www.coe.int/cybercrime
16. Samuel A, Bassey O, Samuel I (2012) Graduate Turnout and Graduate Employment in Nigeria. International Journal of Humanities and Social Science, 2: 258. http://www.ijhssnet.com/journals/Vol_2_No_14_Special_Issue_July_2012/30.pdf
17. Aminu ZS, Zehadul Karim AHM (2016) Youth Unemployment and Poverty in Nigeria: A threat to sustainable Growth and Development. International Journal of scientific research and management (IJSRM) 4: 9. http://www.ijsrm.in/v4-i12/2%20ijsrm.pdf