International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 8, July 2016

ISSN: 2394-4404

Mitigation Of Security Challenges In E-Banking System In Nigeria

DR. Benedict Mbanefo Emewu

Department of Computer Science Ebonyi State University,
Abakaliki

***Abstract:** The advancement in technology has brought various means to elevate human effort in doing things with the use of computer, especially in the area of buying and selling. This advancement with numerous benefits is not without challenges. Electronic banking is simply the use of computers with the internet to carry out banking transactions such as withdrawals through cash dispensers or transfer of funds at point of sale as well as depositing money. The e-banking constitutes an electronic alternative network of payments and benefit of services. The problem with the existing system is that despite the benefit of electronic banking, it also faced with some challenges like phishing, cyber crime, and electronic spam mail etc. The banks that are activated in the Internet are susceptible mainly to the systematic, law part and to the reputational risk and the customers of the electronic banking channel are puzzled concerning to the subject of safety of their transactions and personal data. This survey paper has discussed various security challenges in Nigeria e-banking, various counter measures to mitigate being at risk of uncertainty in carrying out transaction online.*

***Keywords:** Proxy Server, Passcode, IVR, Phishing, e-banking.*

I. INTRODUCTION

E-banking also known as internet banking, or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking that was the traditional way customer's access banking services. Fundamentally and in mechanism, online banking, internet banking and e-banking use the same mechanism of operation via the internet. It is not surprising the

To access a financial institution's online banking facility, a customer with internet access would need to register with the institution for the service, and set up a password and other credentials for customer verification.

Before the emergence of modern banking system, banking operation was manually done which lead to a slowdown in settlement of transactions. This manual system involves posting transactions from one ledger to another which human handles. Figures or counting of money which should be done through computers or electronic machine were computed and counted manually which were not 100% accurate thereby resulting to human errors. Most bank then use only one computer in carrying out transactions which ameliorate the sluggish nature of banking transaction.

E-banking is the banking of new era. This had broken down the time and space barriers. The new banks are providing some of the services exclusively through ATM's.

The introduction of electronic banking services has posed a serious risk on the security of the system due to the presence of spammer and hacker i.e cybercrime and thus several suggestions on how to tackle such threats will be discussed in this seminar work.

A. MOTIVATION

With the modern trend in technology-banking makes it possible for banking customers to access and make cash transactions online without necessary visiting the bank, but the risk of cybercrimes such as phishing, electronic spam mails sets in and has lead to banking customers ignorantly sending their confidential information to spammers who the overwrite their information and sometimes withdraw their money without their notice.

This led to the underlying study to analyze and bring to fore the overall concepts of security challenges facing electronic banking system in Nigeria.

B. OVERVIEW/STRUCTURE

The term Internet Banking or E-Banking Internet both are used as supplement. Making banking products and other services available to wholesale and retail customers, through an electronic distribution channel is called e-banking. In other words E-Banking refers to the banking operations, which is done over World Wide Web.

E-banking is the outcome of technological innovations and competition. In fact, banks have been using electronic and telecommunication networks for delivering a wide range of value added products and services. The devices have been telephone, personal computers including Automated Teller Machines (ATM). The delivery channels have been direct dial up connections, private and public networks. To this newer edition of e-banking are being added e.g. Internet banking and mobile banking. The use of ATM's lead to the concept of 'anywhere' and 'anytime' banking. Through the use of ATM cards, one can operate his bank account to withdraw money from any of bank's ATM installed or available at the nearest site.

The aim of this seminar is to evaluate the prospects of electronic banking in Nigerian banking industry. It also seeks to examine the challenges facing electronic banking in Nigeria and also suggest how to tackle these challenges.

The scope of this seminar is limited to the prospects and suggestions to security challenges in e-banking system in Nigeria.

This seminar work is structured into four sections. Section is introduction, this section discusses the relevance of the topic, section two discusses the related topics, section three discusses the content of the research, and section four is conclusion.

II. LITERATURE REVIEW

A. OVERVIEW OF E-BANKING

Timothy (2012), electronic banking refers to the use of the Internet as a remote delivery channel for providing services, such as opening a deposit account, transferring funds among different accounts and electronic bill presentment and payment. This can be offered in two main ways. First, an existing bank with physical offices can establish a Website and offer these services to its customers in addition to its traditional delivery channels. Second, is to establish a virtual bank, where the computer server is housed in an office that serves as the legal address of such a bank. Virtual banks offer their customers the ability to make deposits and withdraw funds via ATMs (Automated Teller Machines) or other remote delivery channels owned by other institutions, for which a service fee is incurred. Ahasanul (2009) Electronic banking (e-banking) is the newest delivery channel of banking services.

Timothy (2012) posits that three or four decades ago, banking was a simple business; consumers saved their money with and received their financial services from banks. When customers open savings account, they received passbook from the bank with which the account would be operated; and when it is a current accounts, they received cheque books for the same purpose. Today, the banking industry has moved into an era of menu-driven ultra robust specialized software programmes called banking applications. These applications can carry out virtually all banking functions relying heavily on information collection, storage, transfer and processing The application of electronic banking products/services to banking operations has become a subject of fundamental importance and concerns to all banks operating within Nigeria and indeed a condition for local and global competiveness (Ezeoha, 2006; Ikechukwu, 2000). The recent consolidation exercise in Nigerian banking sector has drawn the attention of many banks to application of various technological devices in promoting/achieving better customer service delivery that guaranteed customer satisfaction that translates into increase profitability and higher return on investment.

Timothy (2012), customer's satisfaction holds the potential for increasing an organization's customer base, increase the use of more volatile customer mix and increase the firm's reputation. Consequently, obtaining competitive advantage is secured through intelligent identification and satisfaction of customer's needs better and sooner than competitors and sustenance of customer's satisfaction through better products/services. Technology is then essential in providing faster and more efficient services to customers.

Technology acquisition must be based on actual needs and the proven ability to deliver customer – friendly solutions. But with globalization, Nigerian banks have no choice but to adopt electronic banking services to enhance effective service delivery that transcends to customer satisfaction, if they really want to stay in the business race, let alone be profitable (Madueme, 2009).

But it should be realized that electronic banking services is a brain child of Information and Communication Technology (ICT) that made it possible for service providers and their customers in developing economies to enjoy a good semblance of the services enjoyed in the developed societies. Electronic banking services have afforded banks the opportunities to impress customers which encourage them to keep coming back.

Today, it would be difficult to see any bank in the country that does not render one form of electronic banking service or the other, even banks in the most remote parts of the world.

B. VARIOUS FORMS OF E-BANKING

There are various forms of e-banking which include:

Internet banking, Automated teller machines, tele banking, smart card, debit card, E-cheque ,direct deposit, electronic bill payment, electronic check conversion, cash value stored etc.

a. INTERNET BANKING

Internet Banking lets you handle many banking transactions via your personal computer. For instance, you may use your computer to view your account balance, request transfers between accounts, and pay bills electronically. Internet banking system and method in which a personal computer is connected by a network service provider directly to a host computer system of a bank such that customer service requests can be processed automatically without need for intervention by customer service representatives. The system is capable of distinguishing between those customer service requests which are capable of automated fulfilment and those requests which require handling by a customer service representative. The system is integrated with the host computer system of the bank so that the remote banking customer can access other automated services of the bank. The method of the invention includes the steps of inputting a customer banking request from among a menu of banking requests at a remote personnel computer; transmitting the banking requests to a host computer over a network; receiving the request at the host computer; identifying the type of customer banking request received; automatic logging of the service request, comparing the received request to a stored table of request types, each of the request types having an attribute to indicate whether the request 4 E-BANKING type is capable of being fulfilled by a customer service representative or by an automated system; and, depending upon the attribute, directing the request either to a queue for handling by a customer service representative or to a queue for processing by an automated system.

b. AUTOMATED TELLER MACHINES (ATM)

An unattended electronic machine in a public place, connected to a data system and related equipment and activated by a bank customer to obtain cash withdrawals and other banking services. Also called automatic teller machine, cash machine; Also called money machine. An automated teller machine or automatic teller machine (ATM) is an electronic computerized telecommunications device that allows a financial institution's customers to directly use a secure method of communication to access their bank accounts, order or make cash withdrawals (or cash advances using a credit card) and check their account balances without the need for a human bank teller (or cashier in the UK). Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts, top up their mobile phones' pre-paid accounts or even buy postage stamps. On most modern ATMs, the customer identifies him or herself by inserting a plastic card with a magnetic stripe or a plastic smartcard with a chip, that contains his or her account number.

The customer then verifies their identity by entering a passcode, often referred to as a PIN (Personal Identification Number) of four or more digits. Upon successful entry of the PIN, the customer may perform a transaction. If the number is entered incorrectly several times in a row (usually three attempts per card insertion), some ATMs will attempt retain the card as a security precaution to prevent an unauthorised user from discovering the PIN by guesswork. Captured cards are often destroyed if the ATM owner is not the card issuing bank, as noncustomer's identities cannot be reliably confirmed. The Indian market today has approximately more than 17,000 ATM's.

c. TELE BANKING

Undertaking a host of banking related services including financial transactions from the convenience of customers chosen place anywhere across the GLOBE and any time of date and night has now been made possible by introducing on-line Telebanking services. By dialing the given Telebanking number through a landline or a mobile from anywhere, the customer can access his account and by following the user-friendly menu, entire banking can be done through Interactive Voice Response (IVR) system. With sufficient numbers of hunting lines made available, customer call will hardly fail. The system is bi-lingual and has following facilities offered 6 E-BANKING

- ✓ Automatic balance voice out for the default account.
- ✓ Balance inquiry and transaction inquiry in all
- ✓ Inquiry of all term deposit account
- ✓ Statement of account by Fax, e-mail or ordinary mail
- ✓ Cheque book request
- ✓ Stop payment which is on-line and instantaneous
- ✓ Transfer of funds with CBS which is automatic and instantaneous
- ✓ Utility Bill Payments
- ✓ Renewal of term deposit which is automatic and instantaneous
- ✓ Voice out of last five transactions.

d. SMART CARD

A smart card usually contains an embedded 8-bit microprocessor (a kind of computer chip). The microprocessor is under a contact pad on one side of the card. Think of the microprocessor as replacing the usual magnetic stripe present on a credit card or debit card. The microprocessor on the smart card is there for security. The host computer and card reader actually "talk" to the 7 E-BANKING microprocessor. The microprocessor enforces access to the data on the card. The chips in these cards are capable of many kinds of transactions. For example, a person could make purchases from their credit account, debit account or from a stored account value that's reload able. The enhanced memory and processing capacity of the smart card is many times that of traditional magnetic-stripe cards and can accommodate several different applications on a single card. It can also hold identification information, which means no more shuffling through cards in the wallet to find the right one -- the Smart Card will be the only one needed. Smart cards can also be used with a smart card reader attachment to a personal computer to authenticate a user. Smart cards are much more popular in Europe than in the U.S. In Europe the health insurance and banking industries use smart cards extensively. Every German citizen has a smart card for health insurance. Even though smart cards have been around in their modern form for at least a decade, they are just starting to take off in the U.S.

e. DEBIT CARD

Debit cards are also known as check cards. Debit cards look like credit cards or ATM (automated teller machine) cards, but operate like cash or a personal check. Debit cards are different from credit 8 E-BANKING cards. While a credit card is a way to "pay later," a debit card is a way to "pay now." When you use a debit card, your money is quickly deducted from your checking or savings account. Debit cards are accepted at many locations, including grocery stores, retail stores, gasoline stations, and restaurants. You can use your card anywhere merchants display your card's brand name or logo. They offer an alternative to carrying a check book or cash.

f. E-CHEQUE

An e-Cheque is the electronic version or representation of paper cheque. • The Information and Legal Framework on the E-Cheque is the same as that of the paper cheque's. • It can now be used in place of paper cheques to do any and all remote transactions. • An E-cheque work the same way a cheque does, the cheque writer "writes" the e-Cheque using one of many types of electronic devices and "gives" the e-Cheque to the payee electronically. The payee "deposits" the Electronic Cheque receives credit, and the payee's bank "clears" the e-Cheque to 9 E-BANKING the paying bank. The paying bank validates the e-Cheque and then "charges" the check writer's account for the check.

III. EVALUATION

A. SECURITY CHALLANGES IN E-BANKING SYSTEM IN NIGERIA

The major security issue facing E- banking in Nigeria is Cybercrime which represents a major concern for business executives not only in Nigeria but also in other parts of Africa. In Nigeria, for instance, the banks that have implemented high- tech security system for online banking have however, fallen victims of security breach, and this poses serious impediments to economic activities and business in the banking milieu.

With e-banking gaining ground in Nigeria, customers and online buyers are more likely to face great risk of unknowingly passing on their information to fraudsters. "Hackers" get information of those who have made purchases through websites and then make fake cards which they use with less detection.

a. CYBER CRIME

By definition, Cybercrime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet.

Types of Cyber Crime

Cyber crime activity seems to be an open-ended list of security issues, prominent among them is; Phishing, Electronic Spam Mails, Cyber Stalking, Fake copycat website, Man in the Middle, Man in the Browser.

✓ PHISHING

Phishing is simply a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions. Phishing is usually a social engineering crime pervasive in attacking organizations' or individuals' (customers') information systems (IS) in order to gather private information to be used against organizations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts.

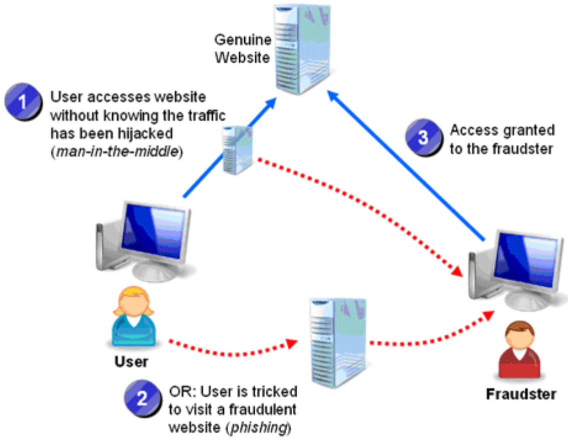
According to recent estimates from the Anti- Phishing Working group phishing scams remain a relatively small percentage of spam sent worldwide today. Phishing attempts to pose significant dangers for unsuspecting victims. It has become one of the fastest-growing worldwide threats on the Internet. This rapid growth has made combating it a huge priority for electronic mail service providers, since phishing impacts every aspect of the Internet and computing and there is no single action from any one company or organization to solve the problem. The remedy can only come in a holistic fashion involving collaboration between technology innovation, industry, government, and user education as prescriptive guidance. To build systems shielding users from fraudulent websites, designers need to know which attack strategies work and why. What makes a web site credible? This question has been addressed extensively by researchers in computer-human interaction. Successful phishing must not only present a high credibility web presence to its victims; it must create a presence that is so impressive that it causes the victim to fail to recognize security measures installed in web browsers. Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites. About two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 2003.

In phishing e-mail messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters "spoof," or mimic, a reputable company. The companies spoofed most often are financial services- Internet organizations such as the GT Bank, First Bank, Citibank, Master Card, eBay, PayPal, etc. Retailers and Internet service providers are also targeted. These phishing e-mails are usually mass mailed. Many of the recipients are not customers of the spoofed companies and may quickly realize that the e-mail is fraudulent, or may believe that the e-mail was mistakenly sent to them and ignore the e-mail. Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam. The scammers claim to be from reputable companies and go to great lengths to emulate the company's visible branding. Their fraudulent e-mails often contain the company's logo and use similar fonts and colour schemes as those used on the company's web site.

Some of the fraudulent e-mails simply reference images from the legitimate company's site. The main link in a fraudulent e-mail sends the recipient to the fraudulent phishing web site, but many fraudulent e-mails include other links that send the recipient to sections of the real company's web site. To further convince the recipient that the e-mail originated from the reputable company, the scammers use a “from” e-mail address that appears to be from the company by using the company’s domain name (e.g., @firstbank.com, @gtbank.com). Phishing e-mails also try to assure the recipient that the transaction is secured in hopes of gaining the recipient’s trust.

In Nigeria, the most recent phishing attacks were on the customers of Inter-switch, which remains the organization with the highest customer base in electronic transactions. The Nigeria Deposit Insurance Corporation (NDIC) disclosed in its 2007 annual report and statement of account that underhand deals by bank staff, among others, resulted in attempted fraud cases totalling over N10.01 billion (over 65 million USD) and actual losses of N2.76 billion (13 million USD) in 2007.

Based on the present situation in the world economy and the appropriate technology, fraudulent action is most likely to increase and phishing remains one of the main means of performing “fraud without borders.” The extent of readiness to stem phishing in Nigeria needs to be determined because fraudulent activities emanating from these nations have far-reaching consequences beyond her borders.


Genuine Website
1 User accesses website without knowing the traffic has been hijacked (man-in-the-middle)
3 Access granted to the fraudster
User
Fraudster
2 OR: User is tricked to visit a fraudulent website (phishing)

Source: www.massivealliance.com

Figure 1: Illustration of Phishing

✓ ELECTRONIC SPAM MAILS

These are unsolicited bulk e-mail sent to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, web search engines, and blogs. Spamming is popular because the advertisers have no operating costs beyond the management of their mailing lists and it is difficult to hold senders accountable for their mass mailings. As a result, costs such as lost productivity and fraud are borne by the public and by Internet service providers that have been forced to add extra capacity to cope with the deluge.

✓ FAKE COPY-CAT WEB SITES

Fake Copy Cat Websites is another recent trend in on-line fraud; the emergence of fake ‘copy-cat’ web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster’s personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

✓ MAN IN THE MIDDLE

This is a form of security breach where the attacker has the opportunity to eavesdrop by making an independent connection with the victims and relays messages between the victim and his bank, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

✓ MAN IN THE BROWSER

This is a form of internet threat related to man in the middle. It’s a proxy Trojan horse that infects a web browser by taking advantage of vulnerabilities in the browser security to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and the host web application. This Trojan horse has been frequently used as a tool to perpetuate E-banking fraud.

B. COUNTER MEASURES

✓ SECURITY OFFICERS SEGREGATION

There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems.

✓ USE OF LOGICAL ACCESS CONTROL

Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.

✓ USE OF PROXY SERVER

Banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank’s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert.

✓ USE OF DIAL UP SERVICES

All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.

- ✓ DISABLING OF TELNET

All unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled.

The application server should be isolated from the e-mail server.

Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats.

Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy.

- ✓ BIOMETRIC

Biometrics in banking also helps to increase customer trust and improve brand reputation. The necessity for a stronger authentication solution became inevitable in banking services because of the growing pace of sophisticated transactional technology adoption along with the unfortunate rise in fraud and security breaches due to reliance on traditional security systems such as passwords.

- ✓ SURVEILLANCE CAMERA

As part of our security services for banks, we offer specialized security systems for ATMs. These systems may include CCTV-Video ATM security cameras to monitor and record activity as well as security alarm systems to signal authorities in the instance of a threat.

IV. CONCLUSION

E-banking offers a higher level of convenience for managing one's finances even from one's bedroom. However, it continues to present challenges to the financial security and personal privacy. Many people have had their account details compromised, as a result of online banking.

This seminar has been able to outline the various types of cybercrimes which is the main security challenge of electronic banking in Nigeria and has suggested the possible means of tackling this security challenges.

Thus, if one is going to use it for financial transactions, he should be aware of the risks involved. Awareness of the risks and problems stressed by this seminar work will enables him/her to take precautions for a more secured online banking experience.

V. RECOMMENDATION

I strongly recommend that Banks should use the proxy server type of firewall so that there will be no direct connection between the Internet and the bank's system.

REFERENCES

[1] Ahasanul, H., (2009); "Issues of E-banking Transaction: An Empirical Investigation on Malaysian Customers Perception", *Journal of Applied Sciences*, (2009).

[2] Ikechukwu, G., (2000); ''Enhancing the Performance of Banking Operations through Appropriate Information Technology in Nigeria Banking Industry, Ibadan: Spectrum Books'', (2000).

[3] Ikechukwu, G., (2000); ''Enhancing the Performance of Banking Operations through Appropriate Information Technology in Nigeria Banking Industry, Ibadan: Spectrum Books''.

[4] Madueme, I.S., (2009); ''*International Journal of Economics and Development''* Banking Efficiency and information Technology in Nigeria: An Empirical Investigation. (2009).

[5] Mahdi, A. and Zhila A., (2008); "Islamic Banking Practice and Satisfaction: Empirical Evidence from Iran", ACRM Journal of Business and Management Research.

[6] Mohammed, S. K. and Siba S. M., (2009); "Service Quality Evaluation in Internet Banking: An Empirical Study in India", International Journal of Indian Culture and Business Management.

[7] Ovia, J., (2010) "Internet Banking: Practices and Potentials in Nigeria", A paper presented at a seminar organised by the Institute of Chartered Accountants of Nigeria (ICAN) Lagos Sheraton Hotel & Towers, Ikeja.

[8] Sharma K. and Singh A.J., (2010); ''*Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering*. Nemati'', Biometric Security in the E World.

[9] Timothy A. T., (2005); ''*International Journal of Business and Management Tomorrow''* Electronic Banking Services and Customer Satisfaction in the Nigerian.