International Journal of Computer Applications Technology and Research
Volume 4– Issue 11, 823 - 828, 2015, ISSN:- 2319–8656

An Empirical Analysis of Security on Nigerian's Internet Banking Platform: an end user's Perspective

Simon Enoch Yusuf
Federal University, Kashere
Gombe State
Nigeria

Abstract: The speedy advancement of Internet business has stirred-up the banking and financial sectors towards encouraging customers to embark on banking on the internet. On the other hand, confidentiality, security, and privacy of online banking activities and users basic information are the main concerns for both the online banking customers and to the banking industry. In this study, we investigated security on Nigerian's internet banking platform of 10 selected financial institutions in Nigeria. The research finding uses a modified security checklist to analyse the security features and reliability of the Nigerian's selected banking industry. The results shows sufficient strength in all the basic security features available on the various internet banking platform, however, few of the platform are not sufficiently fault tolerant built.

Keywords: Electronic banking; Phishing; Online; Privacy, Reliability; Authentication

1. INTRODUCTION

The ubiquitous nature of the internet has caused Nigerian banks to conduct daily banking activities from anywhere easily and conveniently over the internet. The development in the information technology sector and also the development in the banking industry has drastically increased communication and transactions between banks and customers [1].

The speedy advancement of Internet business has stirred-up the banking and financial sectors towards encouraging customers to embark on banking on the internet. This latest banking environment; Internet banking is increasingly managed as an operational activity and an important component of a multi-channel strategy [2]. Internet banking is defined as the use of the Internet to deliver banking activities such as funds transfer, paying bills, viewing current and savings account balance, paying mortgages and purchasing financial instruments and certificates of deposits [3] [4].

Technology based banking is now bringing more choices than ever before in the financial sector. It is now becoming possible to access our bank account in multiple ways and take care of our financial affairs quickly and efficiently [5].

Confidentiality, privacy and security of internet banking transactions and personal information are the major concerns for both the banking industry and internet banking customers [6] [7] [8][9]. Security threats such as keyloggers, phishing, pharming, adware, malware, Trojans, viruses and spyware are currently the most common online banking security threats and risks [6] [7].

Majority of published research on internet banking majorly focused on security on the network side and on also on the server's side by creating a safe and secured communication channels for the user computer and the bank server's side computer [10] and most of the attacks on Internet Banking used today are based on fraudulent internet users stealing users login data.

In Nigeria, identity fraud is the most common type of attack on the internet banking platform [11]. This identity fraud is called phishing and pharming. Others include; Cross-site scripting and Keylogger/Trojan horses. In this type of attack, a software is use to manipulate legitimate user to transact with fake banking platform [11].

One of the most recent types of internet attack is the man-in-the-browser (MITB) attack [12], in this attack, malwares lives inside customers internet browsers, it then changes what customers see on their browser, with this, the attackers now has the ability to steal and modify the destination account number, amount and any information that the customer entered and display whatever they choose.

Generally, Phishing, Adware, pharming, keylogger, malware, spyware, Trojans and viruses are the most frequent online banking security threats and risks [13] available on the internet banking platform.

2. RELATED WORK

As the electronic banking market matures, Internet Banking as well as Mobile Banking has shifted from being merely a distribution channel towards becoming a central part of the bank's growth strategy. Banks have increasingly started to view and leverage their Internet Banking and/or Mobile Banking platform as their new virtual branch, through which (almost) the same services can be delivered to the client as via a physical branch [14].

Hamid et al. [15] Compared and analysed the internet banking system in Malaysia and Thailand. In their analysis, they used comparison as the theoretical base and secondary data to determine the differences between both countries with respect to Internet banking. Their analysis indicates that both nations are dissimilar in providing basic services offered by their commercial banks.

Subsorn and Limwiriyakul [16] Examined Internet banking security systems in Australian banks by creating a proposed Internet banking security. The following were uncovered by their research work; lack of Internet banking security in all the 16 selected Australian bank, Better Internet banking security

information, two-factor authentication and stronger encryption in use by those banks reviewed.

In another paper, Subsorn and Limwiriyakul [7] examined 12 (twelve) Thai commercial banks, they revealed that there was a distinct lack of internet banking security information provided on all the selected Thai banks' websites as compared to the selected Australian banks which provided better internet banking security information.

Mueni and Muchiri [17] used multi case study design to define a framework that can be used for assessing Internet banking system reliability. They collected data from a key informant using a questionnaire and document analysis guide and analysed using both descriptive and inferential statistics. In their study, they found out that documentation and size internal properties had significant positive effect on reliability.

An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia was also conducted by [8]. They examined Internet banking security in nine (9) foreign subsidiary banks in Australia, they compared their results and findings with a previous research [16] [7] in order to produce a more practical and comprehensive guideline, as well as to include a weight rating of security related website information for the banking industry in Australia. The findings of both the previous research paper [16] [7] [18] revealed that there was lack of related Internet banking security information in all the selected Australian owned and foreign owned banks' websites which have the potential to impact on the confidentiality of the banks and its customers as well as future potential customers.

3. METHODOLOGY

This study applied a qualitative research method by employing analytical methods. The Analysis was conducted by investigating the availability and reliability of internet banking in Nigeria. The basic features deployed by each bank were also considered.

Currently, there are 1662 financial institutions in Nigeria, which comprises of 726 Bureau De Change, 21 Commercial banks, 1 non interest bank, 5 Development finance, 3 Discount House, 64 Finance company, 2 Merchant Banks, 792 Microfinance Bank, 1 Microfinance institution, 40 Primary mortgage institution, 7 unclassified financial institutions [19].

The research was carried out in Nigeria – North East. It involved a sample size of seven (7) commercial banks and three (3) Microfinance banks. Three (3) branch from each selected bank was randomly selected and ten (10) IT experts from those banks who were interviewed to determine their perspective of the level of availability and reliability provided.

Sources of data included both primary and secondary data which assisted the researcher to make a thorough analysis of the study problem at hand.

Primary data was collected through personal interviews and use of questionnaires to gather accurate information. While, Secondary data was obtained from available sources such as text books, journals, on-line published articles, information from the local newspapers and internet search engines among others.

In addition, a security checklist by [20] was adopted and modified for the purposes of evaluating the security features of the selected banks. A list of the checklist is presented below:

Table 1. Modified Subsorn & Limwiriyakul Security Checklist.

	Category	Descriptions
1	General online security, privacy and reliability	Provide internet banking security information Privacy in transaction Bank security mechanism system
2	Fault Tolerant	Operate despite failure Roll back in case of system failure Use of redundant system Reliability in terms of accepting wrong input Internet banking system is recoverable from errors and failure Meeting required software standards
3	Security features on the internet banking platform	Required standard for inactivity system timeout Not meeting the required standard for inactivity system time out. Inactivity system timeout not in use Limited daily online transfer amount to third party Limit can be increase by approval of the bank No limit for internet transfer. Login information alert i. last login ii. activity log iii. SMS or email alert login not available Use session management Do not use session management
4	Authentication Technology	User Site Password login restriction Enforce good password practice (combining letters, numbers, and special characters) Enforce login pin length Uses two factor authentication for transaction e.g. addition of Token, SMS etc. Two factor authentication not in use Logon requirement: using user ID, email address, password, CAPTCHA etc 3 times logon failure limitations Logon failure limitation not use On screen logon user input Keypad logon user input Bank site Use of encryption and digital technology
5	IT Assistance, Support and Monitoring	Provide 24/7 customer care line 24/7 customer care line not available Uses secured email Provide frequent ask question support form Monitor internet banking transaction
6	System Requirement	Internet banking platform compatible with popular web browsers. Security software tools available to customers

3.1 Analysis

Table 2. Availability of internet banking features

		Commercial Banks							Microfinance Banks		
S/N	Security feature category	First Bank Plc	Zenith Bank	GT Bank	UBA	Diamond Bank	EcoBank	Sky Bank	Gombe Microfinance Bank Limited	Jewel Coop Microfinance Bank Limited	Adamawa Savings & Loans Limited
1	General online security, privacy and reliability								NA	NA	NA
	a. Provide internet banking security information	✓	✓	✓	✓	✓	✓	✓			
	b. Privacy in transaction	✓	✓	✓	✓	✓	✓	✓			
	c. Bank security mechanism system	✓	✓	✓	✓	✓	✓	✓			
2	Fault Tolerant										
	a. Operate despite failure	✓	✓	✓	✓	✓	✓	✓			
	b. Roll back in case of system failure										
	c. Use of redundant system										
	d. Reliability in terms of accepting wrong input	✓	✓	✓	✓	✓	✓	✓			
	e. Internet banking system is recoverable from errors and failure	✓	✓	✓	✓	✓	✓	✓			
3	Security features on the internet banking platform								NA	NA	NA
	a. Required standard for inactivity system timeout	✓	✓	✓	✓	✓	✓	✓			
	b. Not meeting the required standard for inactivity system time out.								✓	✓	✓
	c. Inactivity system timeout not in use								✓	✓	✓
	d. Limited daily online transfer amount to third party	✓	✓	✓	✓	✓	✓	✓			
	e. Limit can be increase by approval of the bank	✓	✓	✓	✓	✓	✓	✓			
	f. No limit for internet transfer.										
	g. Login information alert										
	i. last login	✓	✓	✓	✓	✓	✓	✓			
	ii. activity log	✓	✓	✓	✓	✓	✓	✓			

	iii. SMS or email alert login	✓	✓	✓	✓	✓	✓	✓			
	iv. not available								✓	✓	✓
	h. Use session management	✓	✓	✓	✓	✓	✓	✓			
	i. Do not use session management								✓	✓	✓
4	Authentication Technology								NA	NA	NA
	User Site										
	a. Password login restriction	✓	✓	✓	✓	✓	✓	✓			
	b. Enforce good password practice (combining letters, numbers, and special characters)	✓	✓	✓	✓	✓	✓	✓			
	c. Enforce login pin length	✓	✓	✓	✓	✓	✓	✓			
	d. Uses two factor authentication for transaction e.g. addition of Token, SMS etc.	✓	✓	✓	✓	✓	✓	✓			
	e. Two factor authentication not in use										
	f. Logon requirement: using user ID, email address, password, CAPTCHA etc	✓	✓	✓	✓	✓	✓	✓			
	g. 3 times logon failure limitations	✓	✓	✓	✓	✓	✓	✓			
	h. Logon failure limitation not use										
	i. On screen logon user input			✓	✓			✓			
	Keypad logon user input	✓	✓			✓	✓				
	Bank site										
	a. Use of encryption and digital technology	✓	✓	✓	✓	✓	✓	✓			
5	IT Assistance, Support and Monitoring										
	a. Provide 24/7 customer care line	✓	✓	✓	✓	✓	✓	✓			
	b. 24/7 customer care line not available										
	c. Uses secured email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	d. Provide frequent ask question support form	✓	✓	✓	✓	✓	✓	✓			
	e. Monitor internet banking transaction	✓	✓	✓	✓	✓	✓	✓			
6	System Requirement										
	a. Internet banking platform compatible with popular web browsers.	✓	✓	✓	✓	✓	✓	✓	NA	NA	NA
	b. Security software tools available to customers										
	c. Meeting required software	✓	✓	✓	✓	✓	✓	✓			

	standards										

Note: NA – Not Available ✓ -Yes

3.2. General online security, privacy and reliability

All the selected commercial banks provide basic internet security tips through email, SMS and their bank web pages. In addition, other security mechanism that provides extra layer of security on the internet platform was communicated to the end-user. However, all selected Microfinance banks do not provide such services and therefore, not available.

3.3. Fault Tolerant

Seven (7) selected commercial institution were examined for fault tolerant capability in terms of failure and reliability. None of the banks provide roll back capability in terms of failure. However, they all have supporting or redundant system in case of system failure and meets the requirement in terms of continuity despite inputting wrong input.

3.4. Security features on the internet banking platform

All selected commercial banks provide inactivity system timeout capability which happen atmost 3 minutes of inactivity. As part of their security features, a limit transfer amount of N1,000,000.00 to third part account in another bank per transaction is enforced on all platform. All banks equally provide last login information, activity login over a period of time, SMS or email alert login information and also session time out.

3.5. Authentication Technology

The following authentication technology is enforce by all the internet banking platform, password login restriction, two factor authentication, 3 times logon failure limitation, use of encryption and digital technology for transaction. However, only 3 of the bank uses on screen logon user password input.

3.6. IT Assistance, Support and Monitoring

Customers care and monitoring banking service is been provided by Nigeria commercial banks to her customers all through the week 24/7. They also monitor all internet transactions on their platform. In addition, FAQ is been used online to support and help bank customers in getting answers to some of their questions.

3.7. System Requirements

All the banks declared that they do not provide security software for their customer uses. They also declared that their internet platform is compatible to all popular browsers, however, one (1) stated that it bank only allow Firefox for it internet banking, they disabled other browsers for security purposes.

4. Conclusions

Implementing appropriate sets of control, polices, processes, procedures, legal framework, software and hardware functions, and organizational structures will assist in achieving greater level of security on internet banking platform. These holistic approach need to be monitored, reviewed, established, implemented, and improved, where necessary, to ensure that the specific security and business objectives of the bank are met.

All selected commercial banks are currently actively using internet banking for transaction with sufficient level of security on their various platforms. However, for additional security on the use of keyboard for user input on the internet platform, the use of on screen logon should be adopted. This is because, hackers use a tool to capture keyboard key strokes and then later use it for illegitimate transaction.

Unfortunately, all the existing selected Microfinance bank do not use internet banking from the user end and therefore analyzing those banks was not possible. Finally, financial institutions are encourage to always meet up with all the novel security challenges in an online banking transaction by continuous monitoring of latest threat on the banking platform and also by increasing the various security features available.

5. ACKNOWLEDGMENTS

I wish to express my deep appreciation and sincere thanks to all Information Technology Personnel's in the various selected Banks for providing us with all the necessary and basic information needed to complete this paper.

6. REFERENCES

[1] Giannakoudi. S. 1999 "Internet banking: the digital voyage of banking and money in cyberspace" Information and Communication Technology Law, Vol. 8 No. 3, pp. 205-43.

[2] Black, N.J., Lockett, A., Winklhofer, H and McKechnie, S. 2002 "Modelling consumer choice of distribution channels: An illustration from financial services. The International Journal of Bank Marketing, 20(4): 161-173.

[3] Singhal, D. and Padhmanabhan, V. 2008 "A Study on Customer Perception Towards internet Banking: Identifying major contributing factors. The Journal of Nepalese Business Studies: V (1), 101 – 111.

[4] Haque, A., Ahmad, H. I., and Daraz, A. H. 2009. "Issues of E – Banking transaction: An Empirical Investigation on Malaysian Customers perception" Journal of Applied Sciences, 9(10), 1870 – 1879.

[5] Aychiluhim, D. and Tibebe, B. 2014 "Internet Banking Security Framework: The case of Ethiopian Banking Industry" HiLCoE Journal of Computer Science and Technology, Vol. 2, No. 2. Pp. 7 – 13.

[6] Subsorn, P., and Limwiriyakul, S. 2011 "A comparative analysis of the security of Internet banking in Australia: A customer perspective" Presented in 2nd International Cyber Resilience Conference (ICR2011). Perth, Australia: Edith Cowan University, 2011a.

[7] Subsorn, P. and Limwiriyakul, S. 2011. "A comparative analysis of internet banking security in Thailand: A customer perspective" Presenting in 3rd International Social Science, Engineering and Energy Conference 2011b (ISEEC2011). Nakhon Pathom, Thailand.

[8] Hutchinson, D. and Warren, M. 2003 "Security for Internet banking: A framework" Logistics Information Management, 16(1), 64 -73.

[9] Hutchinson,D. and Warren, M. 2001 "A framework of security authentication for internet banking" Paper presented at the International We-B Conference (2nd), Perth.

[10] Peotta,L. and Holtz, M. D. 2011 "A formal Classification of Internet Banking Attacks and Vulnerabilities",

International Journal of Computer Science and Information Technology (IJCSIT), Vol. 3, No 1, Feb .

[11] Yusuf, S. E. , Adebayo, K. J. and Adetula, E. O. 2013 "Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique" International Journal of Advanced Computer Science and Applications (IJACSA) Vol. 4, No. 3. pp 156 – 164. Available online athttp://www.thesai.org/Downloads/Volume4No3/Paper_25-Mitigating_Cyber_Identity_Fraud_using_Advanced_Multi_Anti-Phishing_Technique.pdf

[12] Cain, C. "Analyzing Man-in-the-Browser (MITB) Attacks" SANS Institute InfoSec Reading Room, 2014. Available online at https://www.sans.org/reading-room/whitepapers/forensics/analyzing-man-in-the-browser-mitb-attacks-35687

[13] BankMuscat. "Internet banking security threats" Retrieved October, 2015, from http://www.bankmuscat.com/enus/ConsumerBanking/bankingchannels/internetbanking/Pages/InternetBankingSecurityThreats.aspx

[14] Dijkstra, M. and Esajas, M. O. "Security for Internet Banking and in Mobile Banking is the key to Customer Loyalty", retrieved July, 2015, Available online at ww.ibis-management.com.

[15] Hamid, M. R. A., Amin, H., Lada, S., Ahmad, N. 2007 "A Comparative Analysis of Internet Banking in Malaysia and Thailand. Journal of Internet business" Issue 4

[16] Subsorn, P. and Limwiriyakul, S. A. 2012 "Comparative analysis of the security of Internet banking in Australia: A customer perspective". Procedia Engineering 32. Elsevier 260 – 272. www.sciencedirect.com

[17] Mueni, M. F. and Muchiri, M. G. 2014. "An assessment framework for Internet banking system reliability" International Journal of Technology in Computer Science & Engineering, Volume 1(3) , September 2014 , pp 88-100.

[18] Subsorn, P.and Limwiriyakul, S. 2012 "An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia: A Customer Perspective" (IJCSI) International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2.

[19] Central Bank of Nigeria, "Financial Institution" Retrieved August, 2015, from http://www.cenbank.org/Supervision/Inst-DM.asp

[20] Stawowski, M. "Client side Vulnerability Assessment", retrieved from http://www.clico.pl/services/Clientside_Vulnerability_Assessment.pdf, Last accessed on 10/09/2015.