Global Forum for African Studies (GLOFASE) - Volume 2 No 2 June 2014
IP INDEXING ISSN: 119-0133

4

THE ONLINE SECURITY CHALLENGES IN THE CASHLESS ECONOMY OF NIGERIA.

Mullah, Nanlir Sallau
GSE Department
F. C. E Pankshin, Plateau State.
mullakns@yahoo.com

Abstract
Transacting businesses online is gaining momentum in Nigeria. However, this online transaction is threatened by security challenges associated with it. Online transaction is only performed on a system that is networked and is connected to the internet as well. The network connectivity makes all the systems on the network vulnerable to attack. This paper seeks to find out how secured the online transaction businesses in Nigeria are and the person(s) responsible for securing the system. The paper also lists some security tips that will help users from failing victims of online fraudsters and hackers. The paper concludes that, the service providers (banks) and the persons carrying out the transactions are all Stakeholders in securing the system.

Keywords: Positive and negative aspects of cash-less economy, common security breaches on the internet, mis-configuration of the victim host

INTRODUCTION

No matter your field of study, you cannot help but notice the impact that the internet has on our society. It is likely that in no distance future, the Internet will become an important and functional part of our lives (Mark, 2001). Individuals, governments and organizations now routinely connect their computers to the Internet to communicate, provide services, and access massive stores of shared information. It has opened up opportunities and markets that everybody seeks to have. In the developed society, virtually everything seems to be done online and Nigeria is not left out in this struggle, hence, the introduction of cashless economy. The predominant question on the minds of many is does it imply total withdrawal of cash? The simple answer to this question is NO. However; a cashless economy is an economy that minimizes the use of cash by providing alternative channels for making payments online. After all, money is not necessarily physical cash; — but money is what money does. Better still; a cashless economy is an environment in which money is spent without being physically carried from one person to the other. Futurists have been

speculating about the prospects for a cashless society for many years, and such predictions became more frequent following the introduction of "smart" cards—cards containing a computer chip—in the mid-1970s (Gerald,1996). A smart card or electronic purse or wallet is electronic information that is transmitted to a device which reveals the information about how much a person has stored in the bank and how much he can spend (Enesi, 2013). It is commonly known in Nigeria as ATM cards. The ability to purchase goods across borders is fostered with the ease of instant payment not necessarily with physical cash but electronic cash, for example purchases made online at Amazon and e-bay, further driving the world into a global village. Besides the ease of purchasing goods and paying for services that can be done within and outside one's geographical location, another major drive towards the cashless society is cash management. The Central Bank of Nigeria (CBN) has introduced a new policy on cash-based transactions which stipulates a 'cash handling charge' on daily cash withdrawals or cash deposits that exceed N500,000 for Individuals and N3,000,000 for Corporate bodies (CBN, 2011). The new policy on cash-based transactions (withdrawals & deposits) in banks, aims at reducing (not eliminating) the amount of physical cash (coins and notes) circulating in the economy, and encouraging more electronic-based transactions (payments for goods, services, transfers, etc.) These online activities, many conducted beyond national boundaries, have opened up enormous opportunities for security attacks such as identity thefts, computer hackings, privacy breaches, technical sabotages, etc. As with any new technology, there is always a positive and negative aspect associated with it.

POSTIVE ASPECTS OF CASHLESS ECONOMY

A variety of benefits are expected to be derived by various stakeholders from an increased utilization of online transaction systems in any country. These include:

To drive development and modernization of our payment system in line with Nigeria's vision 2020 goal of being amongst the top 20 economies by the year 2020.

To reduce the cost of banking services (including cost of credit) and drive financial inclusion by providing more efficient transaction options and greater reach.

To improve the effectiveness of monetary policy in managing inflation and driving economic growth (Oguwale, Atanda, & Butu-onakoya, 2013).

THE NEGATIVE ASPECTS OF CASHLESS ECONOMY

The obvious negative side is the huge security risk that is now posed to so many organizations and other users alike, yet few people and companies are truly aware of the potential danger. It is like getting in a brand new car and driving down the road at 100km/h, only to realize that the engineers did not equip the car with breaks. If this did occur and a large number of people bought the car, the net result would be a high number of fatalities because the proper breaking was not built into the car. The same thing is occurring with the Internet. Now that individuals, organizations and government have invested millions of naira in this new infrastructure, they realize that security was not properly built in, and now their entire networks are vulnerable (Eric, 2001).The challenges facing the introduction of cashless system in Nigerian economy include the following among others:

1. Network Reliability: Instability of Point of Sale (PoS) networks, which is prevalent

across all operators, would pose a problem or serve as a barrier to usage especially when money sent is not received when needed - which is crucial.

2. Fraud: A prevalent fraudulent act among ATM scammers is likely to occur on the point of sale channel.

3. Security: Concerns were also raised about trust in the Agents providing cash-in and cash-out services, this could be risky for customers and the agents if there is no form of security.

5. System Stability: Fear of the unknown - the current banking crisis (both deposit money banks and microfinance banks) has not helped in allaying the public's fear.

6. Literacy Issues: This is a situation where not all targeted populace were literate, and some of them do not know how to make use of the e-banking. For instance, a dubious businessman may see a customer that do not know how to operate the PoS terminal and decided to deduct more than what the person consume.

7. Network Operator Provider: Most people were anxious to know if this will be done by an existing or a new Point of Sale (POS) service provider. Some people were concerned about usage in rural areas, especially where there is currently no network coverage in terms of money transfer.

8. Inadequate Infrastructural Development: Lack of infrastructural development particularly energy (power) puts a lot of constraints to the operations of e-payment machines (Nwankwo & Eze, 2013).

Common security breaches on the internet

In order to carry out online transactions, the system (Smart cards, computers, ATMs or POS) must be connected to the internet. A computer network is a technological web where several computers, systems, and devices are interconnected with each other. Generally, a computer network relates to a group of computers which are interlinked with each other in order to share resources and information. Its most significant uses are data storage and communication. It does not only include desktop or laptop computers, but also several technical and electronic devices which are required to serve the purpose of data sharing, data transmission, and data communication. It comprises equipment such as web servers, databases, perplexed wiring, cables, and connections, and many other advanced devices. All major operations in a computer network are controlled from a place known as the data center, which is the server room. The Internet is also a kind of network, and is, undoubtedly, the largest, which is why it is known as the network of networks. In order to conduct commerce on the Net, you must be assured of some reasonable level of data security.

The two most common reasons for security breaches:

Misconfiguration of the victim host

System flaws or deficiency of vendor response

Misconfiguration of the Victim Host

The primary reason for security breaches is misconfiguration of the victim host. Plainly stated, most operating systems ship in an insecure state. There are two manifestations of this phenomenon, which I classify as active and passive states of insecurity in shipped software.

The Active State

The active state of insecurity in shipped software primarily involves network utilities. Certain network utilities, when enabled, create serious security risks. Many software

products ship with these options enabled. The resulting risks remain until the system administrator deactivates or properly configures the utility in question.
A good example would be network printing options (the capability of printing over an Ethernet or the Internet). These options might be enabled in a fresh install, leaving the system insecure. It is up to the system administrator (or user) to disable these utilities. However, to disable them, the administrator (or user) must first know of their existence.
Active state problems are easily remedied. The solution is to turn off (or properly configure) the offending utility or service. Typical examples of active state problems include: Network printing utilities, File-sharing utilities, Default passwords, and Sample networking programs.

The Passive State
The passive state involves operating systems with built-in security utilities. These utilities can be quite effective when enabled, but remain worthless until the system administrator activates them. In the passive state, these utilities are never activated, usually because the user is unaware that they exist. Again, the source of the problem is the same. The user or system administrator lacks adequate knowledge of the system.
You will notice that both active and passive states of insecurity in software result from the consumer's lack of knowledge (not from any vendor's act or omission). This is an education issue, and education is the reason for this paper. Education issues are matters entirely within your control. That is, you can eliminate these problems by providing yourself or your associates with adequate education. Put another way, crackers can gain most effectively by attacking networks where such knowledge is lacking.

System Flaws or Deficiency of Vendor Response
System flaws or deficiency of vendor response are matters beyond the end-user's control. These factors are the second most common source of security problems. It's sufficient to say that a system flaw is any element of a program that causes the program to
Work improperly (under either normal or extreme conditions).
Allow crackers to exploit that weakness (or improper operation) to damage or gain control of a System.

WHO IS RESPONSIBLE FOR SECURING THE NETWORK?
The security of electronic cash cannot be left in the hands of financial institutions alone. A Careful look at the source of security breach on electronic cash over the decades points to sources such as from third-party processor of payment data (Aladenusi & Azike, 2011). Even POS machines, as small as they may look, come with their own set of security challenges. POS devices are usually based on standard PC architecture; therefore they share much vulnerability like weak or default configurations, missing security patches and weak password and account policies.
A stand alone system is less vulnerable to security attack but cannot be use for any online transaction. This is to say a system must be connected to a network in order to permits one to perform the online transaction we are talking about here. Users can determine if the site they are using is secured by noting the “secure” icon at the bottom of their browser window.

Also, the address bar of Internet browsers will carry the “https” prefix instead of the standard “http” prefix when the site is secured. It is possible to clone ATM cards, clone a website, hack into or completely take the website down. As we strive to catch-up with technological innovation in advanced countries, we also need to brace up to the challenges inherent with such technologies. The following comprehensive guide and tips are geared towards making us conscious of the dangers out there and what to do to protect ourselves from online criminals (Okereke, 2012).

Be careful what you do on a computer especially a public computer like cyber cafe. When you use a public computer from a cyber cafe to check your emails, ensure you uncheck the 'keep me signed or logged in' box before you sign in to your online accounts. Failure to do this means your email/online account can still be opened even after you sign or log out. And very importantly, after downloading sensitive documents, ensure you clear the download folder otherwise your downloaded document will still be there after you have gone.

These days, websites can be cloned. It is safer to personally enter the Universal Resource Locator (URL) of the website you want to visit on the address bar than to Google it.

Beware of text messages or even calls supposedly originating from a particular phone number or company you think you are familiar with. If it looks too good to be true, it is.

Use strong passwords and change it as frequently as possible. Eschew using such things as your date of birth as passwords. Mix letters, numerals, capital and lower case letters if possible. Example 'JosIsTheCapitalOfPlateauState'. Yes, it is a long one but also easy to remember. Most importantly, it is STRONG, cannot be easily cracked.

Be careful who you send or email your curriculum Vitae (CV) and important documents to. Armed with all these information about you, what else do some criminally-minded people out there need to claim to be you or 'clone' you.

Beware the type of information you leave on social networking sites such as facebook, twitter, beebo, hi5, 2go etc. Be careful who you allow as your 'friend' or socialize with on facebook etc.

Have manifold email addresses. You can dedicate one of the emails for social activities-networking and all that. Another one can be for your financial transactions and may be a third one for career-related transactions. The reason for this is that if the email for social activities is compromised, it will not affect the sensitive information in your career or business emails.

Phone browsing has more security implications than browsing on a typical desk top or laptop computer. It may interest you to know that Google officially admitted that more than 90% of android phones have mobile software with serious security vulnerabilities (Gahran, 2011). It is advisable to install a mobile security antivirus on your smart phone.

Regularly updating your computer also makes it more secured. Similar to this is also to update your web browsers as older versions may be riddled with security flaws. Avoid downloading or opening programs or files if you are not sure of the sites authenticity or credibility.

RECOMMENDATIONS

In order to sustain this policy of cashless economy in Nigeria, I recommend that proper sensitization is required in terms of awareness and the security issues involved. Especially for low income group, who are currently deeply rooted in using cash and see it as a convenient and easy way of receiving and making payments. The sensitization exercise

would require the combined efforts of various stakeholders, including government, financial institutions, clergy, teachers and above all the IT professionals, etc. There should be improvement in infrastructural development so as to enhance the online transactions and thwart the effort of online fraudsters. Government should subsidise computer security products (Antivirus, Firewall etc), and IT products (computers and software) and make them available. When these are properly implemented, Nigeria is ready for full implementation of cashless economy with minimal risk.

CONCLUSION

The transition to a cashless economy will raise a lot of security issues in our financial institutions. Information Technology professionals and non-professionals should help by giving people orientation or awareness on the risks associated with online transactions and the necessary precautions. Information Technology professionals should be ready to provide a robust Information Technology support. Therefore, the indigenous professionals should rise up to this challenge and support the banks on making the policy a huge success.

References

Aladenusi, T & Azike, A. (2011). Cashless Society: Is Nigeria ready for the information security challenges? http://www.vanguardngr.com

Enesi L. (2013, July 20). Online transaction: ICT discussion [blog post]. Retrieved from http://sowinfocomtech.com/blog/2013/06/20/hello-world/

Eric C. (2011) *Hackers Beware*; New Riders Publishing

Gerald S.(1996).The Electronic Purse: An Overview of Recent Developments and Policy Issues. Sourced from: http://www.bankofcanada.ca/1996/01/research/technical-report- no74/

Gahran A. (2011) *Mobile phone security*: what are the risks? Retieved from edition.cnn.com/2011/TECH/mobile/06/17/mobile.security.gahran/

http://www.vanguardngr.com/2011/12/ cashless-society-is-nigeria-ready-for-the-information-security-challenges/ Central Bank of Nigeria(2011): Sourced from cenbank.com.ng

Mark,T (2001).*Maximum Security*: *A Hacker's Guide to Protecting Your InternetSite and Network* . Indianapolis. Sams Publishing.

Nwankwo,O & Eze, O (2013). Electronic Payment in Cashless Economy of Nigeria: Problems and Prospect. Journal of management research. Retrieved from http://www.macrothink.org/journal/index.php/jmr/ article/view/2650/2434

Oguwale, M. Atanda, A & Butu-Onakoya (2013). effect of cashless policy on payment system in tertiary institutions: evidence from olabisi onabanjo university.

Okereke D. (2012) : *cyber security awareness & tips for Nigerians*. Sourced from http://www.nairaland.com/1048039/cyber-security-awareness-tips-nigerians.

Pavol, C. (2002). *Crack Proof Your Software*; San Francisco. No Starch press, Inc.

Scisco, Peter. "Electronic Commerce." Microsoft® Student 2008 [DVD]. Redmond, WA: Microsoft Corporation, 2007.