Awareness of Online/Internet Frauds and Control Measures in Business Environment: Nigerian Experience

Jim Ernest Uwaneze

Abstract*- Advances in technology have affected every aspect of business environment around the world. The effects are generally felt in education, science, commerce, business and particularly the electronic world. These new technologies have facilitated new business procedures from traditional banking and commerce to the electronic (Online/internet) service. The use of online /internet services has helped in ensuring that business activities and banking functions were made as simple as possible. But notwithstanding, people have used online services for fraudulent purpose which individuals need to be aware. Some internet frauds are; banking fraud, phishing, scams, spams schemes and mule recruitment etc. It was recommended that customers should be aware that certain e-mail and messages sent were fake and that Banks should executed more customers education programmes to create wider awareness of the criminal tricks occurred in the internet.*

Keywords: generally felt in education, science, commerce, business and particularly the electronic world, Online/internet, fraudulent purpose, banking fraud, phishing, scams, spams schemes and mule recruitment.

I. INTRODUCTION

Iwundu (2005) stated that recently, technological advancement in the world has enormous impact on most business enterprises. Consequently, banks and other financial institutions in Nigeria seemed to be doing everything to ensure that their functions were made as simple as possible. They also strived to reduce the stress and complexities faced by customers in their banking and business transactions (Onyebu, 2011).

According to Benjamin (2010), investment companies should be aware of internet methodology and audit transactions to prevent the loss of funds. Most online banking fraud schemes involve two steps. First, the criminal steals the customers identity by obtaining the customers account access data, i.e. logon name and password upon succeeding in that endeavor, the criminal uses this information to transfer money to other accounts and to withdraw the funds. To ensure the stealing of a customers identity, criminal have employed different schemes in the past. Furthermore, "the over the shoulder looking" Scheme occurs when a customer performs financial transactions while being observed by a criminal (Benjamin, 2010). A great number of cases have been reported where customers account access data was obtained by the criminal just by observing customers at a public internet access point or an ATM site (Milichamp, 2000).

Obayi, Obi and Okafor (2012) defined business environment as anything, which surrounds the business organization. It affects the decisions, strategies process and performances of the business. Umebali (1997) sees a business as an economic institution, which is primarily engaged in production and marking of goods and services. It involves all economic activities carried out in order to provide goods and services, which could be private or public. Furthermore, business can be defined as an economic institution which is legally engaged in production and marketing of goods and services with the main aim of making profit in the case of private enterprises and social welfare distribution in the case of public sector (Obayi, Obi and Okafor, 2012) **Online/Internet Frauds**.

The term online fraud refers to any type of fraud scheme that uses email, website, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme (Benjamin, 2010). Some forms of online fraud, as stated by Benjamin (2010) include. Internet banking fraud, phishing, mule recruitment, shopping and action site fraud, scams and spams.

II. SCAMS

"Nigeria letter" or 419 scams, as well as "lottery or Spanish lottery" scams, attempt to hire victims into a type of fraud know as illegal advance fee. They typically arrive via email. Criminals send out millions of these fraudulent spam email to random email addresses in the hope of enticing someone to respond. Although the stories in these scams vary widely. After an initial exchange of conversation or emails with the victims, they all usually asked victims to provide bank account or personal detail in order to receive a fictitious financial windfall (Milichamp, 2000).

The promised windfall may be lottery winnings, a huge inheritance, a multi-million dollar bank transfer, etc. While the windfall payment is never made, victims pay large sum of money to cover various false cost and fees (Benjamin, 2010). As a general rule, apply the standard "physical world" test to any online proposition. If it sounds too good to be true, it probably is.

III. SPAM

Spam is unsolicited commercial message sent via email, SMS, MMS and other similar electronic messaging media. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details (Hollander, Denna and Owen, 2001).

Manuscript Received on March 2015.

Jim Ernest Uwaneze, Department of Technology and Vocational Education, Enugu State University of Science and Technology Enugu, Nigeria.

IV. IDENTITY THEFT

A large part of online rime is now centered on identity theft which fraud specifically refers to the theft and use of personal identifying information of an actual person, as opposed to the use of fictitious identity. This can include the theft and use of identity personal information of persons either living or dead. Strategies for prevention of computer and electronic bank frauds are as follows: You can stay safe by following common sense and a few basic simple roles; Do not keep password on your computer, do not pay attention to get-rich on your schemes, never give your password to someone else, never send people money that contacted you via email or any other method in the internet especially etc. (world bank, 2000) **phishing**.

The public nature of the internet has made it vulnerable to a lot of security threats. It therefore requires a systematic approach to guarantee its security and integrity in such areas as data transmission, payment confidentiality and the ever pervasive issue of cyber crime (Benjamin, 2010). The objective of such cyber crime usually is to transfer funds illegally from one account to another through the process of phishing and mule recruitment.

In phishing a form of spam is used fraudulently gain access to people’s internet banking detail through the use of spam e-mail purporting to be from a bank. According to Gee (2001). In this way criminal fish for legitimate bank customers log-on information. As well as target online action sites or other online payment facilities. Millions of these fraudulent e-mail are sent by criminals to randomly e-mail addresses in the hope of luring unsuspecting innocent persons into phishing stems from personal bank details. The phishing stems from combining the word “password” and “fishing” criminals send email that appears to be from the customers bank that direct customers to a fake website. In course of confronting education programmes, thereby reducing its effectiveness. It however takes a while before all customers (Milichamp, 2000).

On the other hand, Mule recruitment is the process of getting a person to receive stolen funds using his/her bank account, and then to transfer those funds to his/her cohorts. Criminals usually send out millions of fraudulent job and employment e-mail to random addresses, in the hope of luring unsuspecting persons into their criminal activity. According to Benjamin (2010) Other mule recruitment strategies include ways that online criminals now to launder funds. Here criminals advertise jobs on popular employment or job-seeking websites, in chat rooms or through unsolicited employment e-mail. Depending on the circumstances, mules may also face prosecution. A conviction for an offence of money laundering may carry a penalty of up to 20 years imprisonment in some jurisdictions.

V. CONTROL MEASURES THROUGH SECURITY SCHEMES

Benjamin (2010) listed the following secondary schemes: One time password: Some banks sometimes improve security, by using “one time password”, also, called OTPS. When the customers account is activated for online banking, the bank mails a list of OTPS to the customer. Each time the customer performs a transaction, he enters one OTP for verification. Once used, the OTP becomes invalid. If the customer runs out of OTPS, a new list is sent to him or her while this approach effectively prevents, “over the shoulder looking”, it generally fails to prevent other fraud schemes. Phishing e-mail also ask for OTPS, and a customer have enough to give out his logon name and password will likely also provide OTPS.

Trojans do as well capture the OTPS once entered. At the same time, they falsify the customers input in the browser software (e.g. by adding an invisible character) or cause the browser to crash. This causes the customers transaction to be intercepted and the OTP to still be valid. The criminal can then use this valid OTP to perform a fraudulent transaction.

VI. USE OF HARDWARE TOKEN

The high-tech alternative to paper OTP list are “hardware tokens”. These devise have the form factor of a key chain attachment, featuring a displays a new OTP every 60 seconds. Because each OTP is only valid for a limited period of time, they provide significant protection against “over the shoulder looking” and phishing schemes. Hardware tokens do not however, protect the against Trojans. The fact that the OTP is only valid for a short time just reduces the amount obtained by the Trojan. Because man criminal already use automated scripts on their services to perform fraudulent transactions once the data received from the Trojan, the times limit proves no significant barrier to the criminal Transaction specific OTPs key Generator.

The short come of both paper OTP lists and hardware tokens lies in the fact that each OTP is not transaction specific. That is, the same OTP can be used to verify either a genuine or a fraudulent transaction. One possible way to overcome this flaw is to use a key generator device that generates an OTP based on primary transaction parameters. If a criminal captures such an OTP, he cannot use it for a fraudulent transaction, since this OTP, can only be used to verify a transaction with the same parameters as entered on the key generator transaction monitoring.

A completely different approach to secure online banking comes from thee adaptation of fraud prevention system used with credit and debit card processing. In payment card processing, fraud has been a known phenomenon for many years. Technical security measures introduced to payment cards, such as magnetic strips or chips, have only provided temporary relief from fraud losses. The only measure that proved to limit fraud losses permanently was the deployment of transaction monitoring software. This has become the defects standard for fraud prevention with payment card processing worldwide (Benjamin, 2010).

Transaction monitoring occurs in Bank is data center. For each transaction, the transaction monitoring software scrutinizes the current transacts parameters, and compares it with the previous transaction of both the customer and the counterparty of transaction histories.

VII. RISK SHIELD FRAUD PREVENTION

Banking fraud patterns: A fraud pattern for example can be an unusually high frequency of payments going into one target account from different source accounts. If none of the source accounts have ever transferred funds to this been originated from interrupt programmes (IP) address ranges

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

belonging to certain internet service provider (Milichamp, 2001). At the moment, Risk shield is prevention logic contains about 80 different online banking fraud patterns.

In addition, Risk shield looks out for “unusually” transaction patterns because they could be emerging fraud patterns. Once Risk shield administrators are alerted, they use the Risk shield analysis and simulation environment to isolate potentially new fraud patterns, and simulate the effectiveness of the developed countermeasures (Benjamin, 2010). Also, non monetary transactions, such as password changes address changes or claims of lost card are used by Risk shield to detect specific fraud pattern.

VIII. CONCLUSIONS

Fraudulent is not new in any environment. However, what is relatively new is the involvement of online /internet services in attempting to banking transactions, business transaction, decimate and generalize from what has been transmitted. Banking institutions need to come to terms that all the various criminal elements online/ internet need more and effective preventive and control measures in order to enhance efficiencies and confidence in transactions between the institutions and her customers.

IX. RECOMMENDATIONS

The following recommendations were made:

1. Customers and internets users should be aware that certain e-mail and text messages sent to them were fake.
2. Banks should execute more customers education programmes to create wider awareness of the criminal tricks in the internets
3. Government as well should help in prosecuting any person found on such criminal act without partiality

REFERENCES

[1] Benjamin, M.O. (2010) *Introduction to management information systems and computer based Accounting solutions.* Enugu; Immaculate publications limited.

[2] Hollander, A.S., Dema, E.L & Owen, C.J. (1999) *Accounting information Technology and Business Solution;* 2nd ed. Singapore. McGraw-Hill international Editions.

[3] Iwundu, E.O. (2005) Internet Banking: *A New Innovation in the Banking Industry.* Lagos Longmans Publishers.

[4] Obayi, A.U., Obi, V.A. & Okafor, C.E. (2012) *Entrepreneurial Dynamics.* Owerri. Equity Ventures and Atlas projects Limited.

[5] Gee, P. (2001) *Spicer and pegler’s Book-keeping and Account;* 26th ed. London, Tolley Lexis-Nexis.

[6] Onyebu, C.M. (2011) *Awareness and utilization of internet services by commercial Bank customers in Anambra state.* Journal of Research in science and Technology Education 4(1), 211-218.

[7] Milichamp, A. H. (200) *Auditing;* 7th London; continuum.

[8] Umebali, E.E. 91997) *Management of Small Scale Business, Agribusiness and cooperative Enterprises.* Enugu. Associate.

[9] World Bank (2000) *Information Communication Technology.* A World Bank Group.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.