KOGI JOURNAL OF MANAGEMENT

VOL. 6, No 1, March, 2020

STRATEGIC ACTIONS FOR CONTROLLING INTERNETS FRUADS IN BUSINESS ENVIRONMENT IN RIVERS STATE

[1]Jim, Ernest Uwaneze *PhD.*

[1]87 Ubie Street, Ahoada
Rivers State, Nigeria.
Ernestjim100@gmail.com

Abstract

Advancement in technology have affected every aspect of business environment around the world .The effects are generally felt in education ,sciences, commerce, business and particularly the electronic world . The user of internet services has helped in ensuring that business activities and banking functions were made as simple as possible . But notwithstanding, people have used internet services for fraudulent purpose which individuals needed to be aware. The purpose of this study was to determine the security schemes in controlling internet frauds. This study adopted descriptive research survey design. The populating of the study consists of 60 respondents from five banks and their customers in Rivers State. Structured questionnaire was used to collect data for this study. Two research questions and two null hypotheses were formulated to guide study. Mean with standard deviation was used to analyze the research questions. While t-test was to test null hypotheses at 0.05 level of significance. It was concluded that many people in Rivers State have not yet identified some of the software measures for controlling internet frauds. Based on the conclusion; it was recommended that banks and information communication technology (ICT) training centers should execute more customer's education programme to create wider awareness of the criminal tricks in the internet and there control measures.

Keywords: *Internet Fraud, Business Environment, Rivers State.*

INTRODUCTION

The public nature of the internet has made it vulnerable to a lot of security threats. It therefore requires a systematic approach to guarantees its security and integrity in such areas as data transmission, payment confidentiality and the ever pervasive issue of cybercrime (Benjamin, 2010). The objective of such cybercrime usually is to transfer funds illegally from one account to another through the process of phishing and mule recruitment. 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 transaction (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 customer's identity by obtaining the customer's account access data, i.e. logon name and password upon succeeding in that endeavour, the criminal uses this information to transfer money to other accounts and to withdraw the funds. To ensure the stealing of a customer's identity, criminal have employed different schemes in the past. Furthermore, "the over the shoulder looking" scheme occurs when a customer performs financial transaction while being observed by a criminal (Benjamin, 2010). Great number 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 making 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 good and services with 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). The study focused mainly on banking sectors of business organizations. Bank is a financial institution where money and other valuables are kept for safe custody.

The term online fraud refers to any type of fraud scheme that uses email, web site, 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 (Jim, 2012). Some of online fraud, as stated by Benjamin (2010) includes. Internet banking fraud, phishing, mule recruitment, shopping and action site fraud, scams and spams.

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 emails 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 factious 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 "physical world" test to any online proposition. If it sounds too good to be true, it probably is.

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).

A large part of online crime 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 (Jim, 2015). 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 (World bank, 2000).

In phishing a form of spam is used fraudulently to gain access to people's internet banking detail through the use of spam e-mail purporting to be from a bank. According to incomplete statement 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 this fraudulent e-mail is 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 form the customers bank that direct customers to a fake website. 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. Some banks sometimes improve security, by using both software measures and media measures for controlling internet frauds (Sherman, 2002). He further stated; one time passwords. Hardware Token, Transaction OTPS using key generator, uses of smart card and USB, Tokens transaction monitoring and Risk Shield Fraud prevention as software security measures.

One time password: when the customer's accounts are activated for online banking, the bank mails a list of OTPS to the customers. Each time the customer performs a transaction, he enters one OLTP of r verification. Once used, the OTP becomes invalid. This approach effectively prevents "over the shoulder looking key generators device that generates an OTP based on primary transaction parameters. It has a keypad that lets the customer enter the source account, target account, transaction amount, and a pin. When the online transaction is received by the banks sever, it performs the same calculation as the key generator and thus verifies the OTP. Use of Smart Card and USB Tokens, implement a different approach to authentication. Smart Cards contain Crypto processors without a display. Smart Cards provide a high level or fraud protection for many years. (IMFORM, 2004).

Some media measures for controlling internet frauds as stated by shah (2002). Include: communication and timely access to information to empower management decision making, mitigation of customer vulnerability to fraud by providing adequate customer education, awareness of socio-economic climate, organization of leering for fraud prevention and adaptive policies, procedures and controls.

Statement of the Problems

Certain online/internet fraudulent activities are invoked with the advanced technology. People have used internet services for fraudulent purpose which individuals need to identify and control such practices. Internet frauds are banking fraud, phishing, scam, spam schemes and mule recruitment as identified by Benjamin (2010). Obviously, if these internet fraudulent activities are not prevented duly, it will pose insecurity and lack of confidence in using internet services, also hinders the effective operation of business transactions.

Purpose of the Study

The purpose of the study is to determine the security schemes for controlling internet frauds in Rivers State. Specifically, the study sought to:

1. Determine the software measures for controlling internet frauds.
2. Determine the media measures other controlling internet frauds.

Research Questions

The following research questions guided the study.

1. What are the software measures for controlling internet frauds?
2. What are the medial measures for controlling internet frauds?

METHODS

Descriptive survey research design was adopted to determine the strategic actions for controlling internet/online frauds in rivers state. The populations of the study consisted of 60 respondents with 30 bank staff and 30 bank customers who were randomly selected form five banks in rivers state. The sample banks are First Bank PLC, Zenith Bank, Skye-Bank, Eco-Bank and U.B.A Bank respectively. The structured questionnaire was the instrument used for data collection. Four-point Rating Scale of Strongly Agree (SA), Agree (A), Disagree (D) and Strange Disagree (SD) were used. The validity of the instrument was determined by given draft copies to three experts in computer education and business education departments of Ignatius Ajuru University of Education, Port Harcourt, Rivers State. Test retest method was used to establish the reliability of the instrument. Product moment correlation coefficient was used to determine the reliability of the instrument and obtained the value of 0.82 which is deemed highly reliable the questionnaire was administered and completely retrieved by the researcher and his assistant at spot. The data collected were analyzed using mean with standard deviation for research questions and t-test to test null hypotheses at 0.05 level significance, with a given degree of freedom. Criterion mean value of 2.50 and above is considered agreed; while any mean value below 2.50 is regarded as disagree. For the hypothesis, if the calculated t-value is less than table value, of 1.96 what is the table value & the significance level? Null hypothesis was not rejected but if calculated t-value is greater than equal to the table value of 1.96 of 0.05 level of significance null will be rejected results

Research Question 1

1. What are the software measures for controlling internet frauds in Rivers State?

Table 1: Mean Ratings of Bank Staff and Their Customers on Software Measures for Controlling Internet Frauds in Rivers State.

S/N	Items On Software Measures	Mean (X)	SD	Decision
1.	Use of one time password	3.76	0.58	Agreed
2.	Use of one time password	3.83	0.52	Agreed
3.	Risk shield fraud prevention	3.58	0.51	Agreed
4.	Biometric authentication	3.33	0.48	Agreed
5.	Transaction specific OTPS using key generator	3.58	0.50	Agreed
6.	Organization of seminars/workshops on internet fraudulent activities	3.00	0.42	Agreed
7.	Use of Smart Card and USB	3.30	0.53	Agreed
8.	Transaction Monitoring	3.20	0.42	Agreed
9.	Transaction specific OTPS using key generator	2.93	0.50	Agreed
10.	Fraud prevention software	2.77	0.53	Agreed

11.	Multi-layer passwords	3.31	0.44	Agreed
12.	Using historical data to determine probability of fraud during each transaction	3.22	0.54	Agreed
13.	Strengthening of authentication systems using biometrics	3.11	0.42	Agreed
14.	Data encryption	3.70	0.44	Agreed
15.	Use of specialist third parties for online transactions to enhance confidentiality	3.30	0.49	Agreed
16.	Scalability of security system	3.82	0.59	Agreed
	Grand	**3.35**		**Agreed**

Where, x=mean, SD=Standard Deviation

The result of Table 1 shown that all respondents agreed with item 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, and 16, which indicate all the 16 items are in agreement with software measure for controlling internet frauds in rivers state. The result shows a grand mean of 3.35

Research Question 2

What are the media measures for controlling internet frauds in Rivers State?

Table 2: Mean Ratings of Bank Staff and Their Customers on Media Measures for Controlling Internet Frauds in Rivers State.

S/N	Items On Media Measures	Mean (X)	SD	Decision
1.	Creation of public awareness on security schemes for controlling internet fraud through television	2.73	0.65	Agreed
2.	Creation of public awareness on media control measure through radio	2.61	0.58	Agreed
3.	Creation of public awareness on security schemes for controlling internet frauds through newspaper and magazines	3.00	0.71	Agreed
4.	Customers education programmes	2.86	0.69	Agreed
5.	Organization of seminar/workshops on security schemes for controlling internet frauds	2.52	0.53	Agreed
6.	Communication and timely access to information empower management decision making	2.83	0.64	Agreed
7.	Mitigation of consumer vulnerability to fraud by providing adequate consumer education	2.62	0.53	Agreed
8.	Awareness of socio-economic climate	2.83	0.64	Agreed
9.	Engaging consultants/specialists	2.50	049	Agreed
10.	Organizing learning for fraud prevention to staff	2.54	0.53	Agreed
11.	Multi-layer passwords	3.31	051	Agreed
	Grand	**2.71**		**Agreed**

The data in table 2 revealed that, items 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 were in agreement with the Media measures for controlling internet frauds. Therefore majority of the respondents agreed on the Media measures of security scheme for preventing internet frauds in rivers state. The grand mean value of 2.71 was an indication that most people in rivers state have not applied to current media measures in controlling internet frauds.

Table 3: T-Test Analysis of the Mean Ratings of Bank Staff and their Customers on the Awareness of Internet Frauds in Rivers State.

S/N	GROUPS	N	MEAN (X)	SD	DF	T-CAL	T-CRIT	DECISION
1.	Bank Staff	30	2.82	0.40	58	2.14	1.96	Rejected
2.	Bank Customers	30	2.85					

Where, DF =Degree of Freedom, t-cal= t-calculated, t-crit=t-critical, SD= standard deviation

The result of table 3 revealed that, the calculated t-value of 2.14 greater than the t-critical value of 1.96 at 0.06 level of significant difference on the mean ratings of the respondents on the software measures for controlling internet frauds in rivers state. Hence, the null hypothesis was not rejected.

Table 4: T-Test Analysis of the Mean Ratings of Bank Staff and their Customers on The Awareness of Internet Frauds in Rivers State.

S/N	GROUPS	N	MEAN (X)	SD	DF	T-CAL	T-CRIT	DECISION
1.	Bank Staff	30	3.72	0.42	58	0.83	1.96	Not Rejected
2.	Bank Customers	30	3.53					

The result of table 4 indicated that the calculated t-value of 0.83 is less than the table value of 1.96. Hence, the null hypothesis was not rejected. The result revealed that there is no significant difference in the mean ratings of bank staff and their customers on the media measures for controlling internet frauds in Rivers State.

DISCUSSION OF FINDINGS

The data presented table 1 provided answer to research question one. The findings revealed that most people considered software measures in controlling internet frauds in rivers state such as use of one time passwords, risk shield prevention, creation of public awareness, biometrics authenticity and organization of seminars/workshops. The finding is in consonance with the findings of Sherman (2002) and Shah (2012) that stated these software measures; strengthening biometrics authentication, transaction monitoring, fraud prevention software, data encryption, multi-layer passwords, if properly applied will help in controlling internet frauds in our business environment as well.

The result in table 2 revealed that all items stated were needed media measures for controlling internet frauds in rivers state. The findings indicated that, the followings; customers education programme, creation of public awareness, organization of seminar/workshops, and engaging consultants/specialists may be a useful measure for controlling internet frauds. These findings are in agreement with findings of Jim (2012) and Milichamp (2001) that stated some media measures for controlling internet fraud; such as creation of public awareness through media, organization of seminars and engaging consultants/specialists.

The result of table 3 of null 'hypothesis one showed that there was no significant difference between the mean responses of bank staff and their customers on the software measures for controlling internet frauds. The calculated t-value of 1.14 is less than the critical value of 1.96. Hence, null hypothesis was not rejected. The result of table 4 revealed that there is no significant difference in the mean responses of bank staff and their customers on the media measures for controlling internet frauds in Rivers State. The calculated t-value of 0.83 less than the table value of 1.96 indicated that null hypothesis was not rejected. This finding was in line with the findings of Jim (2015) that shows no significant difference in mean response on awareness of internet frauds in Nigeria.

CONCLUSION

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

Security issues are major barriers to internet banking and e-commerce activities among consumers with fraud highlighted as an important risk associated with payment system. To secure and e-banking system, International Business Machines (IBM) placed emphasis on defining clear objectives. This is achieved by understanding the business goals, objectives and critical success factors when planning the security schemes, as well as the impact on the business if they are not achieved. The issue of communication was found to play an important role in e-banking security in addition to organization flexibility, availability, transparency and security, knowledge and awareness.

RECOMMENDATIONS

Base on the findings and conclusion the following recommendations were made.

1. Bank customers and other internet users should identify that certain e-mail and text messages sent to them were fake.
2. Banks and ICT training centre should execute more customers' education programme 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

Akinyemi Ibidapo, O., Z.O., & Oyelami, O.M. (2010). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. *Intenational journal of electrical & computer sciences, 10, (6) 68-73 available from:* http://search.ebscohost.com/login.aspx?direct=true&db=iih&an=62093371&site=ehost-*live*

Benjamin, M.O. (2010) *Introduction to management information systems and computer based accounting solution. Enugu; Immaculate publications limited.*

Gee, p. (2001) *Spicer and Pegler's Book-Keeping and Account; 26th ed. London, Tolley Lexis-Nexis.*

Hollander, A.S., Dema, E.L & Owen, C.J. (1999) *Accounting Information Technology and Business solution; 2nd ed. Singapore. McGraw Hill International Editions.*

Inform *(2004) how can a Bank prevent Online Banking Fraud? [Online] available at; <http://internetbankingfraud.com/>[accessed26 November 2011]*

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

Jim, E.U. (2012). Utilization of E-learning for effective teaching of vocational education courses in Nigerian tertiary institutions*. Journal of Research in Science and Technology Education. 491), 41-47.*

Jim, E.U. (2015). Awareness of online/internet frauds and control measures in business environment: Nigerian experience *international journals of management and humanities 1(6), 3-5.*

Milichanp, A.H. (200) *Auditing; 7th London; continuum.*

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

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.

Shah, M.H., (2012*). Critical Success factors in e-banking: a study of two UK Retail Banks.*

Sherman, E (2002). Fighting web fraud. Newsweek June 10. [Online] Available at: *<http://www.tlsi.net/articles/newsweek%20_061002.pdf> [Accessed 15 April 2013]*

Umebali, E.E. (1997) *Management of Small Scale Business Agribusiness and Cooperative Enterprises. Enugu. Associate.*