AWARENESS ON DIGITAL SECURITY AND E-BUSINESS IN NIGERIA

Oscar Odiboh[1], Charity Ben-Enukora[2], Toluwalope Oresanya[3], Darlington Yartey[4], Ayoola Aiyelabola[5]

Dept. of Mass Communication, Covenant University, NIGERIA
[1]Dr. odion.odiboh@covenantuniversity.edu.ng
[2]Mrs. enukora.ben@stu.cu.edu.ng
[3]Mr. oresanya.tolulope@stu.cu.edu.ng
[4]Mr. yartey.darlynton@covenantuniversity.edu.ng
[5]Ms. Ayoola.aiyelabola@stu.cu.edu.ng

Abstract

This study examined three fundamental threats to the security of digital business transactions in Nigeria. From experiential and personal perspectives of the people, especially as the enthusiasm for internet usage is acknowledged to be exponential, the study presented a variegated micro community as its locus. It touched on the bullying, stalking and extortions on the internet which fed on local desire to be part of the global technology family. With reference to earlier studies, it was recognized that though digital insecurity is a worldwide phenomenon, its prevalence in Nigeria seemed to have reached higher proportions. Founded on the theoretical platforms of identity flexibility and dissociative anonymity, this study examined the awareness level and experiences of phishing, cloning and hacking by residents of a mixed urban/semi-urban/rural community in Nigeria. Adopting a mixed research methodology, the study primarily implemented a qualitative approach involving thirty-two Focus Group discussants of mixed demographics - four male and four female aged 17-45 years, in four contiguous locations in Ota community. The study engaged a secondary methodology of quantitative survey of two hundred purposively selected adults and consistently focused on the electronic business transaction variable and depended on respondents' willingness to participate, based on a past experience of internet stalking. Victims of either cloning, hacking, or phishing were 55.1% whilst 41.4% suffered damages amongst the respondents. Users' vulnerability which was discovered, necessitated the recommendation of identity protection techniques, mass media awareness campaigns on digital security, as well as integration of digital security education in schools' curriculum in Nigeria.

Keywords: Public awareness, E-business, Digital security, Cloning, Hacking, Phishing, Identity theft, Nigeria.

1. INTRODUCTION

Phishing is a strategy deployed by scammers, sending same message to numerous addresses with the hope of getting the targets to reply to the messages and thereby steal personal information of victims for criminal purposes. Hacking denotes to unlawful copying, removal, interference, intrusion, destruction or manipulation of other people's information on the internet either for revenge or financial gains. Cloning means the creation

of a fake copy of someone's identity information using it to defraud or cause harm to either the original owner or other unsuspecting users.

Phishing, cloning and hacking are prevalent digital security threats through which identity and personal information are stolen on mobile platforms.

With increased number of mobile telephone line subscription and number of cell phone users in Nigeria, business transactions has transformed from physical buying and selling of goods on the streets and open markets to virtual shoping areans on the internet. The buying and selling activities on different internet platforms have captured the interests of criminals who defraud unsuspecting users.

The activity of criminals on the internet not only has a devastating effect on individual victims and the government, it also causes grave damages in the economy. The realities of online fraud are harsh in the business realm, as it affects every aspect of the economy that is represented online (Adeoye, 2016). It has been asserted that "Nigeria loses N89.55 billion (equivalent of 0.80 percent of the nation's Gross Domestic Product) as a result of cybercrime annually" (Ogbodo,2016). The amount of money lost due to phishing, cloning and hacking attacks is enormous and increases each year as Lenardon (2006) argues that "as the criminals' profit grows, so will the attacks".

2. DIGITAL INSECURITY AND E-BUSINESS

Insecurity in e-business platforms have continued to threaten economic activities across the globe. This situation is a serious challenge to Nigerian economy as it hinders public enthusiasm to take advantage of the enormous business opportunities that the internet brings. Security experts have expressed worries that the activities of criminals in digital business sites would cause grave injuries in the future as perpetrators are becoming more sophisticated by the day and extremely difficult to identify for prosecution. Therefore, the protection of business transactions on digital platforms has become increasingly important. The level of digital security awareness amongst Nigerians and knowledge on how to protect their e-business transactions is however not ascertained.

One of the earlier studies in Nigeria regarding digital insecurity Adeniran (2008) emphasizes that the internet has not only facilitated the growth of internet crimes in Nigeria, but has equally enhanced the level of sophistication of related finance-based criminality and modernization of criminality' among the Nigerian youths. In another perspective, Ibikunle and Eweniyi (2013) offered a general overview of Cybercrime and Cyber-security describing the scenario as the evolution of new type of war which will cause destruction of greater magnitude than the two past world wars, if not properly nipped in the bud. Amongst all studies that explored the nature and extent of cybercrime victimization, Ndubueze, Mazindu-Igbo and Okoye (2013) observes that younger respondents, males, married respondents, respondents with higher level of education, unemployed respondents and Christians are more likely to fall victim of cybercrime.

Narrowing down the studies on digital insecurity from foreign contributors, Herley (2012) gave a critical analysis of phishing as a game of binary classification of targets into true positives (targets successfully attacked) and false positives (those that are attacked but yield nothing) the attacker therefore distinguishes internet users. Jakobsson and Young (2005) described a novel type of phishing attack which they labeled distributed phishing attack that is immune to the effects of detection due to a vast collection used by the phishers referring each victim to a unique page. Felt and Wagner (2011) on the other hand, described how the User interfaces for mobile devices makes the users vulnerable to phishing attacks because mobile applications and websites commonly interact in ways that can be spoofed by attackers.

Various publications also dealt with exposition of cybercrime strategies and guides on how it could be detected with suggestions about personal security proofs (Youngsam, Jackie, Damon, Elaine and Markus, 2013; Hutchings and Hennessey, 2009; Bernik, 2014; Levene, 2008). Some analysts have also argued that the regulation of the cyberspace within criminal law lags behind technological development. Following this procession of argument, it may be said that law enforcement officials cannot effectively pursue prosecution of digital criminals without a well-defined cybercrime offences and procedural rules governing evidence-gathering during investigation. Lynch (2005) cited in Hutchings and Hennessey (2009) maintains that "investigation is difficult and costly and there may be reluctance to commence an investigation into a crime that has originated from another jurisdiction, particularly within countries that do not have laws criminalizing their conduct". Furthermore, Wall (2008), cited in Bernik (2014) argues that "there are still problems related to the corroboration of attacks, the cause of damages and the identification of perpetrators, which is why many of such acts remain unreported, unpursued and the perpetrators remain at large".

To provide adequate legal framework for prosecution of internet misdeeds therefore, the Federal Republic of

Nigeria in 2015 took a daring measure by enacting the Cybercrime Prohibition Law which criminalized phishing, cloning and hacking and a host of other internet misdeeds as well as non-disclosure of such acts by victims.

3. OBJECTIVES AND RESEARCH QUESTIONS

The objectives of this study are to:

1. Find out the level of awareness of digital security threats on the internet.
2. Know the rate at which Nigerians are exposed to these Internet crimes and their experiences.
3. Find out the level of repondents' knowledge on how to protect their personal information on the Internet.

These objectives were translated to research questions.

4. METHOD AND MATERIALS

The study adopted both qualitative (Focus Group Discussion in four locations comprising of eight participants each) and quantitative (survey) methods. Two hundred respondents who engage in electronic business transactions participated in the survey study, while 32 participated in Focus Group Disscussion. Only 198 copies of the questionnaire were properly filled and deemed valid for the study. The respondents comprising 97 female and 101 male respondents were selected through purposive sampling technique. Purposive sampling was used because engagement in e-business transactions was the criterion for selection. The questionnaire was self-administered by the researcher and it provided the opportunity of explaining the concepts phishing and cloning to the respondents who do not understand them.

The focus group included eight members each, four male and four female between the ages of 17 – 45 years, in four different locations in Ota community totaling 32 discussants. The discussion was moderated by the researcher to make sure that each discussant contributed to the discussion and each session lasted for 60 minutes. The locations for the FGD were chosen by convenience sampling.

5. THEORECTICAL FRAMEWORK

Deviant behaviours on the virtual business spots involve the interconnected process of Technological Determinism, Social Learning Process, Socio-Economic Pressure, Ready Access to Victims and Identity Flexibility and Dissociative Anonymity and Routine Activity.

According to McLuhan, new technologies bring new changes to the society and consequently affect how the people in that society behave according to Sobowale, Amodu, Aririguzoh, Ekanem (2015). Socio-Economic Factors also play prominent role in internet crimes especially in Nigeria. Studies on the socio-demographic characteristics of internet misdeeds revealed that unemployment and economic sustenance are crucial factors influencing those who engage in criminal activities on digital business platforms as well as the victims who respond to phishing messages with the belief that the outcome will eventually improve their economic status. The intenet guarrantees identity flexibility and dissociative anonymity as well as large

number vulnerable of victims. More so, constant practice and consistency in the game enable the perpetrators become more sophisticated and inflict more damages on victims.

6. RESULTS

All the 32 discussants for the focus group discussion disclosed that they received phishing mails at least twice in one month. According to them, these mails ranges from business proposals and promotions such as offers for sales of goods at low price, auction sales and buy one item to get more products for free.

Three out of 32 discussants said they have been victims of phishing and all of them said they lost cash in the process, while 11 respondents have suffered damages due to hacking attacks more than twice. They disclosed that the inability to operate their accounts and lose of customers were the major challenges they faced.

Five others who were not victims claimed to know some other persons who have been victims of phishing, cloning or hacking, while the remaining 13 discussants were not victims and also had no idea of anyone who has been a victim.

A discussant who was once a victim of phishing, said, “When I received the email alert that I have won 1million naira in Lacasera promo, I thought it was a miracle. In fact, I called the number in the mail and the person I spoke with said I should 50,000 to claim the money. All of us in the house were dancing, praising God that he has remembered us. I did not have the 50,000 naira. So, it was my mother who helped me to borrow money from her friends. I paid the money into their account and I was told to wait for some days for the processing. So, I waited till today, I haven’t heard from that guy that called himself Mr Gbenga”. On the other hand, other victims bought recharge cards and sent the pin numbers to the phishers in place of cash, while the last phishing victim said her fiancée’s account was hacked and the phishers sent mail to him to quickly pay some money into one account number that she was stranded which he did only to realize later that it was a scam.

Furthermore, amongst all discussants only two persons had an informal training on how to protect their personal information on the internet. Thus, majority of the discussants lack adequate knowledge on how to protect their identity when engaging in buying and selling of goods and services on the internet business environment.

TABLE 1: ***Awareness of digital security threats on the internet.***

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	131	66.2	66.2	66.2
	no	34	17.2	17.2	83.3
	can't say	33	16.7	16.7	100.0
	Total	198	100.0	100.0	

Are you aware of the security threats on the internet?

TABLE 2: ***Exposure to phishing, cloning or hacking on internet business platforms***

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	phishing	94	47.5	47.5	47.5
	cloning	3	1.5	1.5	49.0
	hacking	36	18.2	18.2	67.2
	none	38	19.2	19.2	86.4
	phishing & hacking	22	11.1	11.1	97.5
	all	5	2.5	2.5	100.0
	Total	198	100.0	100.0	

How often are you experience these internet crimes?

TABLE 3: *Respondents' victimisation*

		Respondents' sex		
		male	female	Total
If exposed, were you once a victim of any of these internet crimes?	yes	55	54	109
	no	46	43	89
Total		101	97	198

Were you once a victim of any of these internet crimes?

TABLE 4: ***Repondents knowledge on how to protect their personal information on the Internet.***

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	114	57.6	57.6	57.6
	not at all	27	13.6	13.6	71.2
	not really	57	28.8	28.8	100.0
	Total	198	100.0	100.0	

The research findings indicate that majority of the respondents received phishing mails regularly. This confirms Hitchcock(2014) postulations that "If you haven`t yet received a so-called Nigerian scam message by e-mail, you're in a small minority".

On the frequency of victimization, a total of 60 (30.3%) respondents were affected once, amongst them were mainly phishing victims. Those affected more than once were altogether 44 (22.2%) respondents who were mainly victims of hacking. Out of the 104 victims, 82 (41.4%) said they suffered lose in the process, while 22 (11.1%) of the victims did not suffer any lose. Those who lost their customers 31(15.7%) were victims of hacking, those who lost cash were 24 (12.1%) mainly phishing victims, material lose were 4 (2.0%), 9 (4.5%) suffered reputation damage, while 5 (2.5%) respondents suffered reputation damage and lost their customers as well.

Another incredible fact is that many of the victims of such business proposals and sales promotions phishing scams are gullibile individuals. The findings implies that many Nigerians do not have an appropriate sense of the threats that they face as individual Internet users.

The study also found that the discrepancy between their sexes was not quite significant, thus both male and female can be victims. In terms of age groups of victims, the result indicates that respondents within the ages of 20-35 are more likely to fall victims of phishing, hacking and cloning attacks though the margins between those within 20-25 and those between 26-30 years were not significant. This result is in consonance with Ndubueze, Mazindu-Igbo, Okoye (2013) who posit that younger respondents are more likely to become victims. Also, the level of education may not influence victimization as victims with secondary school education were 39, followed by University Graduates who were 28, while those with National Diploma were 15, Post Graduates are 13 and those with the National Certificate in Education were only 8 persons. This result does not support Ndubueze, Mazindu-Igbo, Okoye (2013), who claimed that respondents with higher level of education are more likely to fall victim of cybercrime.

Students topped the list on the victim's occupational disposition, followed by public servants, then traders, artisans, Self-employed victims, unemployed victims and apprentices respectively.

The Focus Group Discussion reveals that some people have gone out of business due to phishing, cloning and hacking attacks on internet business platforms. Persistent victimisation can be attributed to the fact that cyber-attacks information ordinarily is kept secret to avoid blames as well as inadequate awareness and proper knowledge among Nigerians. This implies that Oludare (2016), was right afterall when he noted that "Nigeria remains woefully unaware of the risks that cyber-attacks pose to its economy, national security, and their privacy".

7. CONCLUSION AND RECOMMENDATION

The internet is a truly a wonderful innovation in the history of mankind. It has brought about drastic change in the manner in which business transactions are carried out across the globe. However, the spate of the criminal activities and victimization in the computer-generated business environment has drastically intensified loss of business capital and investments. Dissociative anonymity and identity flexibility of perpetrators of these crimes have continued to pose huge challenges to investigation and prosection.

Lack of knowledge about digital security as well as gullibility and quick wealth syndrome on the part on Nigerians are contributing factors to the spate of crime on e-business platforms.

The mainstream media should devote time and space for digital security programmes for internet business crimes daily reports just as they do for crimes report in the 'real world' and encourage security experts and analysts to partake in educating the public on the need to be cautious so that Nigeria can boast of citizens who can use the internet thoughtfully.

The Nigerian Ministry of Trades and Commerce should sponsor campaign on digital security awareness across the broadcast media to educate Nigerians on security threats they should look out for when they engage in business transactions on the internet and how they should protect themselves or businesses from attacks.

In addition, digital security education should be part of everyday life at all levels of social life starting from the family and be culcated in school curriculum since business transaction on the internet has come to stay. Everyone needs to be educated on how to engage in e-business safely.

ACKNOWLEDGMENT

This paper is funded by Covennant University Centre for Research, Innovation and Development (CUCRID).

REFERENCE LIST

Adeniran, A. I. (2008). The internet and emergence of yahooboys sub-culture in Nigeria. *International journal of cyber criminology* 2, (2); 368–38

Adeoye, T. (January 3, 2016). Nigeria: Online fraud - taming global underworld. Retrieved from http://allafrica.com/stories/201601040664.html,2016,

Bernik, I. (2014). *Cybercrime and cyber warfare*. GB ISTE and John Wiley and son Inc.

Felt, A. & Wagner, D. (2011). "Phishing on mobile devices". Retrieved from http://www.w2spconf.com/2011/papers/felt-mobilephishing.pdf.

Herley, C. (June 1, 2012). Why do Nigerian scammers say they are from Nigeria? Retrieved from research.microsoft.com/pubs/167719/WhyFromNigeria.pdf. 2012.

Hutchings, A. & Hennessey, H. (2009). Routine activity theory and phishing victimization: Who got caught in the net? *Current Issues In Criminal Justice*, 20 (3); 433-451;

Ibikunle, F.& Eweniyi, O.(2013). "Approach to cyber security issues in Nigeria: Challenges and solution". *International Journal of Cognitive Research in Science, Engineering and Education,* 1, (1); 100-110.

Jakobsson & Young (2005). Distributed phishing attacks. Retrieved from Shttps://eprint.iacr.org/2005/091.pdf.

Lenardon, J. (2006). *Identity theft toolkit; how to recover from and avoid identity theft*. International self. counsel press.

Levene, T. (2008). *How to avoid scams*. Age concern books, London.

Ndubueze, I., Mazindu-Igbo, E. & Okoye, O. (2013). "Cybercrime victimization among internet active Nigerians: An analysis of socio demographic correlates. *International Journal Of Criminal Justice Sciences*, 8 (2); 22-34.

Ogbodo, D (2016) Nigeria loses N89.55bn annually through cybercrime". *Thisday* newspaper, 2016, March 30. Retrieved from https://www.thisdaylive.com/index.php/2016/03/30/nigeria-loses-n89-55bn-

annually-through-cybercrime/

Oludare, R. (January 6, 2016). Putting the cybercrime law to test in 2016. Retrieved from https://guardian.ng/features/focus/putting-the-cybercrime-law-to-test-in-2016/

Sobowale,I., Amodu, L., Aririguzoh, S. & Ekanem, T. (2015). "The internet as a tool for information and education: The case of Ota community in Nigeria". In *Edulearn* 15: 7th Annual International Conference on Education and New Learning Technologies, Barcelona. Retrieved from http://eprints.covenantuniversity.edu.ng/5637/1/the%20internet%20as%20a%20tool%20for%20information%20and%20education.pdf

Ugwu, E., Eze, E. O. & Ugbene, I. J. (2012). "On the technological promises and challenges facing e-business in Nigeria". Asian Economic and Financial Review, 5(3); 521-531.

Youngsam, P., Jackie, J., Damon, M., Elaine, S. & Markus,J. (2013). "Scam baiter: Understanding targeted Nigerian scams on Craigslist". *International Journal of Cognitive Research in Science, Engineering and Education,* (1);1-15