IJCJS

Cyber Crime Victimization among Internet active Nigerians: An Analysis of Socio-Demographic Correlates

Philip Nnameziri Ndubueze,[1] Emmanuel Uzodinma Mazindu Igbo,[2] & Uzoma Odera Okoye[3]
University of Nigeria, Nigeria

Abstract

Although Nigeria is one of the top cyber crime prone countries, not many studies have examined the dynamics of cyber crime victimization in Nigeria. This study attempts to feel that gap. It present findings from the analysis of the influence of some socio-demographic variables like age, gender, marital status, education, occupation and religion on cyber crime victimization, using a sample of one thousand three hundred and fifty four (1354) internet-active Nigerians residing in Lagos metropolis. The study found that younger respondents, males, ever married respondents, respondents with higher level of education, unemployed respondents and Christians are more likely to fall victim of cyber crime. The results of this study have significant policy implications for the fight against cyber crime and criminality in Nigeria.

Keywords: Age, Cyber Crime, Education, Gender, Occupation, Religion, Victimization.

Introduction

Cyber crime has become a serious problem in Nigeria, culminating in the listing of Nigeria as third on the roll of the top ten cyber crime hot spots in the world by a 2009 Internet Crime Report (National White Collar Crime Centre and the Federal Bureau of Investigation, 2010). The seriousness of this problem can be better appreciated when we consider the fact that in spite of the several interventions made by Nigerian government and non-governmental organizations in tackling cyber crime, Nigeria has for four consecutive years (2006, 2007, 2008 and 2009) ranked third on the list of world cyber crime perpetrator countries (National White Collar Crime Centre and the Federal Bureau of Investigation, 2010). According to Odapu (2008), cyber crime is at an all time high in Nigeria as cyber café owners, hoteliers and landlords sometimes collaborate with

---

[1] Department of Sociology and Anthropology, University of Nigeria, Nsukka, Enugu State, Nigeria. Email: philipndubeze@yahoo.com
[2] Department of Sociology and Anthropology, University of Nigeria, Nsukka, Enugu State, Nigeria. Email: maziigbo@yahoo.co.uk
[3] Department of Social Work, University of Nigeria, Nsukka, Enugu State, Nigeria. Email: uzokoye@yahoo.co.uk

perpetrators. Despite the efforts of law enforcement agencies to tackle it, cyber crime has become a growing social problem in Nigeria (Ribadu, 2007).

Writers and commentators have argued that full-scale organized cyber crime is fast emerging (Lusthans, 2013). "Systems that people rely upon, from bank to air defense radar, are accessible from cyberspace and can be quickly taken over and knocked out without first defeating a country's traditional defenses" (Clarke & Knake, 2010, p. 31). The growth of information technology and computer connectivity creates space for criminals to exploit security vulnerabilities in the cyber space (Broadhurst, 2006; Kigerl, 2012). Unfortunately, several functionalities of the modern day web browsers are not vulnerability-proof (Agbefu, Hori & Sakurai, 2013), thus exposing the average internet user to cyber crime victimization. With mobile telephony access made pretty easier over the past half a decade in Nigeria through the offering of internet services by virtually all Global System for Mobile Communication (GSM) service providers in Nigeria, the internet has pervaded the lives of many adult Nigerians.

With the increasing dependence on the internet for work, business and pass-time, the internet with all its associated challenges and risks has really come to stay in Nigeria. However, not so many in Nigeria are aware that the internet super high-way has been invaded by criminals and deviants who lurk around desperately looking for targets. Oftentimes, the unguarded, naïve and casual internet user fall prey to their antics. The problem of cyber crime victims is made worst by the seeming inability of law enforcement agents to effectively prosecute offenders. Clearly, law enforcement has not been able to keep up with technological advances to prevent cyber crime (Jaishankar, Pang & Hyde, 2008; Choi, 2006). Anti-hacking laws, because of their traditional approaches to crime containment, have been ineffective (Sharma, 2007). The issue of cyber crime victimization needs to be discussed in detail.

Various studies have explored the nature and extent of cyber crime and victimization (Bossler & Holt, 2010; Choi, 2008; Finn, 2004; Holt & Bossler, 2009; Halder & Jaishankar, 2010; Marcum, 2008; Ngo & Paternoster, 2011). Also there have been quite a number of Nigerian studies on cyber crime. One of the earlier studies by Longe and Chiemeke (2008) examined how access to the internet boosts criminality. Tade and Aliyu (2011) and Ojedokun and Eraye (2012), looked at the Nigerian university undergraduates involvement in internet crime and the benefits they believe that come from it. Other studies like Adeniran (2008) and Aransiola and Asindemade (2011), also focus on cyber crime in Nigeria. Adeniran (2008) argues that the advent of the internet technology in Nigeria has led to the modernization of fraud among the youth in that cyber fraud seems to have become accepted as a means of living for the Nigerian youth. He argued that this is more so for those who are of college age (Adeniran, 2011).

However, very few studies have been done on cyber crime victimization in Nigeria. This is the gap this study hopes to fill. The present study investigates the socio-demographic correlates of cyber crime victimization by seeking answer to the question: What are the factors that can predispose one to cyber crime victimization in Nigeria?

Method

Population and procedure

A study sample of 1500 was drawn from Lagos metropolis using multi-stage sampling approach. The cluster, simple random and availability sampling methods were used in selection of the respondents. The first stage, which is the primary sampling units (PSU) involved the division of Lagos metropolis into 16 enumeration areas or clusters using the list of all the 16 Local Government Areas in Lagos metropolis as a frame. From these 16 clusters, simple random sampling was used to select 10 local government areas. The second stage involved the use of simple random sampling to select 5 cyber cafes from each of the 10 local governments, totalling 50 cyber cafes. The third stage, which is the ultimate sampling units (USU) involved the selection of 30 cyber cafes users from each of the 50 selected cyber cafes to make up 1500 respondents. This was done using purposive sampling method. In each of the chosen (50) cyber cafes, respondents were selected on the basis of availability at the cyber cafes until the required number of 30 respondents were selected. However, only 1354 questionnaires were correctly completed and used for data analysis.

Tool and Sample

The questionnaire was the primary instrument of data collection. The selected sample consisted of 817 males and 537 females given a total of 1354. 1011 of the respondents were single, 323 were currently married while the remaining 20 respondents were widowed, divorced or separated. The youngest respondent was 15 years while the oldest was 57 with a mean age of 32 years. With respect to level of education, 55 respondents completed 6 years of schooling, 709 completed 12 years of schooling, 424 had university education, while the rest had vocational skill qualifications. Majority of the respondents were Christians (810). 756 respondents were students or apprentices while only 73 of them were unemployed the rest had one form of employment or the other.

Measures

To measure cyber crime victimization, respondents were asked the following four questions:

- Have you ever fallen victim of cyber crime before?
- Have you ever received any email asking you to disclose some personal information like your ATM PIN number?
- Have you ever received any email from an unknown person purporting that you have won some money and requesting some personal information or some kind of commitment from you?
- Have you ever replied an email and later discovered it was junk or fraudulent?

These four questions were used as an index for victimization. In building this index, once a respondent answers yes to three out of the four questions, we will then assume that he/she has been a victim of cyber-crime. This index was used in cross tabulating the socio-demographic variables.

Results

Table 1. Distribution of respondents by some Socio–demographic Variables and Cyber crime Victimization (n = 1354)

Variables	Cyber crime victimization			X^2
	Have been victim of cyber crime	Have not been victim of cyber crime	Total	
Age (Years)				p< .069
Younger respondents	226 (18.9)	967(81.1)	1193 (100.0)	
Older respondents	21 (13.0)	140 (87.0)	161 (100.0)	
Gender				p< .197
Male	158 (19.3)	659 (80.7)	817 (100.0)	
Female	89 (16.6)	448 (83.4)	537 (100.0)	
Marital Status				p< .005
Single	167 (16.5)	884 (83.5)	1011 (100.0)	
Ever married	80 (23.3)	263 (76.7)	343 (100.0)	
Level of Education				p< .342
Low level of education	9 (17.3)	43 (82.7)	52 (100.0)	
Medium level of education	151 (17.2)	727(82.8)	878 (100.0)	
High level of education	87 (20.5)	337 (79.5)	424 (100.0)	
Occupation				
Student/Apprentice	114 (15.1)	642 (84.9)	756 (100.0)	p< .000
Business/trading/Artisan	39 (17.3)	187(82.7)	226 (100.0)	
Civil/Public Servant	74 (24.7)	225 (75.3)	299 (100.0)	
Unemployed	20 (27.4)	53 (72.6)	73 (100.0)	
Religion				p< .040
Christian	169 (20.9)	641 (79.1)	810 (100.0)	
Muslim	60 (14.9)	343 (85.1)	403 (100.0)	
African Traditional Religion	4 (17.4)	19 (82.6)	23 (100.0)	
Others	14 (11.9)	104 (88.1)	118 (100.0)	

Note. Younger respondents refer to those 15 – 34 years, while older respondents refer to those 35 years and above. Ever Married respondents refer to those who are married, divorced, separated or widowed. Low education refers to those that had less than seven years of schooling; medium education refers to those that had less than 16 years of schooling, while high education refers to those that had more than 16 years of schooling.

Table 1 indicates that 18.9% of younger respondents (15–34 years) have fallen victim of cyber crime as against 13.0% of older respondents (35 years and above). Younger respondents appear to be more vulnerable to cyber crime victimization than older

respondents though this is not out rightly statistically significant (P< .069). This is hardly surprising as the younger respondents constitute the majority of the students' population/ internet-active group and therefore are more exposed to the risk of victimization than their counterparts. Table 1 also shows that 19.3% of male respondents and 16.6% of female respondents have been victims of cyber crime though this is not statistically significant (P< .197). Again, this could be attributed to the frequency of on-line activities by males. Males stay on-line more than females and sometimes may return late at night from cyber cafes.

Findings also indicate that 16.5% of single and 23.3% of ever married (married, widowed, separated and divorced) respondents had fallen victim of cyber crime. Statistically significant differences also exist among the two groups (P< .005). Ever married respondents appear to have been more victimized than those who are single. This is probably because they visit the cafes less frequently than single respondents and are therefore less likely to be aware of the tactics/tricks of hackers.

A look at the level of education of respondents shows that 17.3% of respondents with low level of education (less than seven years of schooling), 17.2% of those with medium level of education (less that 16 years of schooling) and 20.5% of those with high level of education (More than 15 years of schooling) had been victims of cyber crime. This finding was however not be statistically significant (P< .324). People with higher level of education are more prone to cyber crime victimization than those with low and medium education. This is perhaps so because people with higher level of education use internet facilities less frequently and may not be abreast with emerging cyber threats and hackers strategies.

Cyber crime victimization with respect to occupation indicates that 15.1% of students/apprentice, 17.3% of business people/traders/artisans, 24.7% of civil/public servants and 27.4% of unemployed respondents have fallen victim of cyber crime. Statistically significant difference exist between various occupations (P<.000). Unemployed persons are the most affected category of cyber crime victims. This is perhaps because this category of people are often hooked to the internet, desperately searching for money making opportunities. In their desperation, they are more likely to fall prey to cyber crime victimization.

For religion, 20.9% of Christians, 14.9% of Muslims, 17.4% of African Traditional Religion faithful and 11.9% of other religions like Hindu and Eckankar have fallen victim of cyber crime. The above table suggests that Christians are more likely to fall victim of cyber crime than adherents of other religions (P< .040). This may perhaps be a function of the "logic of numbers" since Christian users appear to be more in number.

The study further investigated the activity mostly engaged in by respondents while on the internet. Findings show that 1, 37.8% pre-occupy themselves with email/chatting when on the internet, 9.2% use the internet for job search, 20.6% use it for academic research, 13.2% for news/entertainment and 2.3% for other activities which include "business" and "sourcing for clients" (see Figure 1). Since students constitute the majority of the internet usage population in Lagos metropolis one would have expected that their major internet activity will be academic research. However, the above finding suggests that students' major pre-occupation online is email/chatting. With the growth of social network sites like Face book, Twitter, Net-log, You-tube, Skype and so on, many students are entering chat rooms and making friends with both known and unknown persons thereby increasing their vulnerability to cyber crime victimization.

Figure 1. Distribution of respondents based on what they use the internet for most of the time
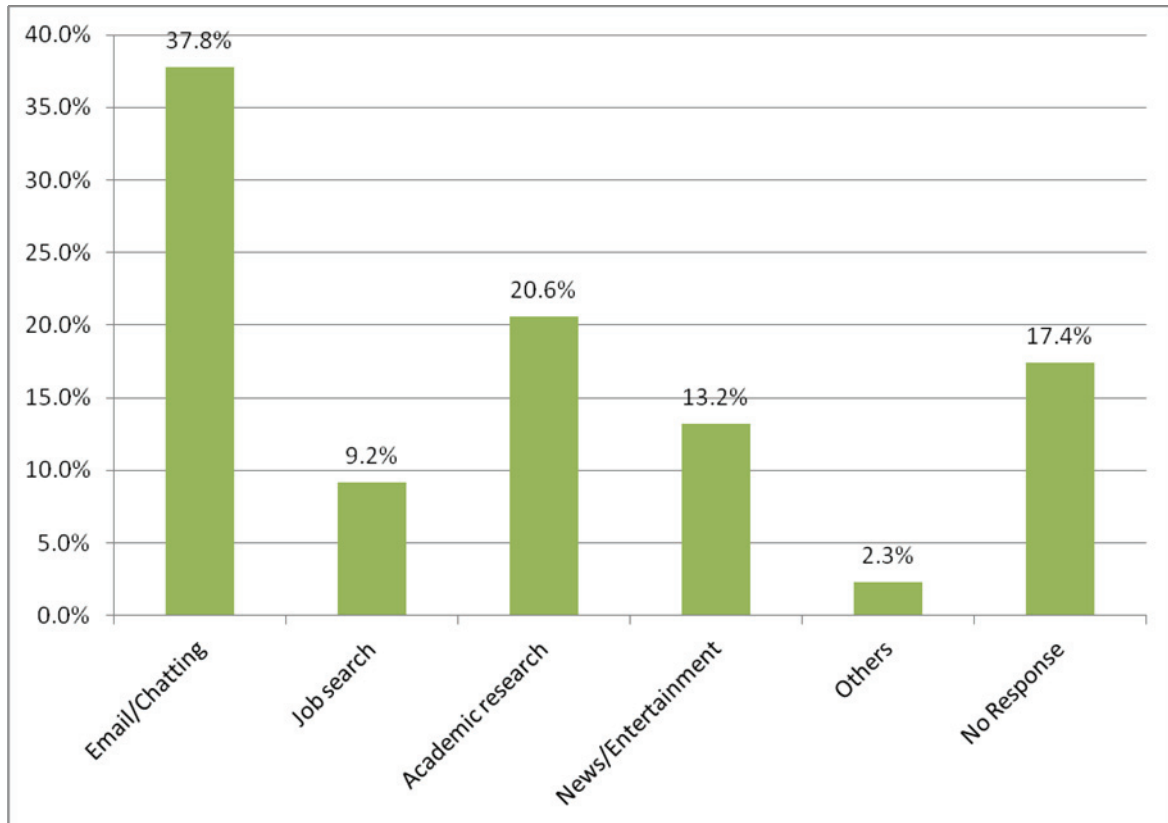

Table 2 indicates that the independent variables are age, sex, marital status, level of education, occupation and religion, while the dependent variable is victimization. The result of the regression analysis shows that three variables: age, occupation and religion were statistically significant ($p<.018$, $p<.002$ and $p<.044$ respectively). The distribution shows that younger respondents are more likely to fall victim of cyber crime than older respondents. Also, unemployed people are more likely to fall victim of cyber crime than people of other occupation and Christians are more likely to fall victim of cyber crime than people of other religions. Therefore, age, occupation and religion are good predictors of cyber crime victimization. Unlike older respondents, younger respondents are more likely to take online risk without calculating it. This is hardly surprising, given that young people's world is a world of adventures. Similarly, unemployed respondents, in their desperation for online job opportunities may be trapped. Because of the relatively high level of youth unemployment in Nigeria, many young job seekers spend quality time on the internet searching for employment and business opportunities thereby exposing themselves to cyber crime victimization. Christians perhaps use the internet more than members of other religious groups and therefore are more exposed to online victimization than the rest of their counterparts.

Table 2. Logistic regression predicting the influence of socio-demographic variables on cyber crime victimization

Socio-Demographic Variables	B	S.E.	Wald	df	Sig.	Exp (B)
Age	.598	.252	5.637	1	.018	1.819
Sex	.145	.150	.931	1	.335	1.156
Marital Status	–.336	.168	3.970	1	.756	.957
Highest Education	–.044	.140	.097	1	.756	.957
Occupation	–.239	.077	9.733	1	.002	.787
Religion	.190	.066	8.237	1	.044	1.209
Constant	1.191	.475	6.284	1	.012	3.290

Discussion

The study found that younger respondents, males, ever married respondents, respondents with higher level of education, unemployed respondents and Christians are more likely to fall victim of cyber crime than the rest of their counterparts. This finding concurs with the long standing association of age with crime in the literature (Stolzenberg, 2008). It is however contrary to that of Ngo, and Paternoster (2011), who found that sex and marital status were not statistically related to cyber crime victimization. Furthermore, the finding agrees with that of Alshalan (2005), who in a study in United States found that males are more likely than females to become victims of cyber-crime so also people who stay longer on the internet. It also agrees with the general pattern in the literature that that establishes gender difference in crime victimization (see for e.g., Fox, Nobels, & Piquero, 2009; Radar & Goodrum, 2010).

Many young people in Nigeria spend all day in the Internet not only due to high rate of unemployment but also as a result of get rich quick syndrome which they feel can happen through the internet (Wada & Odulaja, 2012). The over-emphasis on wealth by the Nigerian society has left the youth with no other choice but to pursue it, albeit by hook or crook. Cyber crime, with its anonymity, speed and relative guarantee of returns, has become pretty fashionable among the youth. With poor recreational facilities, most youth have found a recreational haven of some sort in cyber cafes where they hang out for the better part of their day (Adeniran, 2008; Ayofe & Oluwaseyifunmitan, 2009).

Nigeria is one of those African countries that experienced prolonged military rule and governance challenges which have adversely impacted on her economy. Nigeria also has a high rate of youth unemployment and poor infrastructural development. All of these have left majority of the youth disenchanted, disillusioned and de-motivated. This development has eroded the spirit of patriotism and love for the father land that past Nigerian heroes were famous for. The age-long perception of the male figure as the bread winner of the family is still strong in Nigeria today, thus the "get rich quick" mentality is more prevalent among males than females. The youth are adventurers and will want to try new ideas, however crazy they may be. They are risk-insensitive and will take any risk without weighing the consequences. Furthermore, young adults, do not have much life experience and are often naïve, they are pretty easy to convince or rather confuse. Consequently they are likely to fall prey to the gimmicks and tricks of cyber criminals.

Findings from the study also show that level of education of respondents has no relationship to cyber crime victimization. This finding is supported by the work of Alshalan (2005), who found that education has no effect on cyber victimization. What this points to is that cyber crime victimization cuts across everybody and so should be taken seriously. The present study also found that more respondents used the internet for emailing and chatting more than for academic purposes, especially given the fact that most of the respondents were students. A study by DeBell and Chapman (2003), in the United States, found that of the children and youth, who use the Internet, 72% use it for schoolwork, 65% for e-mailing or instant messaging, and 62% to play games. Another study by Livingstone and Helsper (2007), among young people aged 9-19years, found that Email is the most popular activity (72%) followed by instant messaging (55%). This then means that young people use the internet for purposes other than academic and such other purposes could be crime-related.

While debates on cyber crime and cyber terrorism have dominated several international fora, unfortunately, such debates often times do not fully address the concerns of cyber crime victims (Choi, 2008). In Nigeria today, there is presently no law that is specific to cyber crime, though there are general laws that are not specifically related to cyber crime but are being enforced to deal with the crime (Wada & Odulaja, 2012). However, cyber crime proactive control measures that are relatively inexpensive and more sustainable may be better than reactive measures (McQuade, 2006). According to McQuade (2006) cyber crime can be minimized through public enlightenment campaigns, formal education, and professional training.

Conclusion

Cyber crime problem has become a global problem and so is the plight of its victims. This study found that marital status, occupation and religion are good predictors of cyber crime victimization. Cyber criminals are intelligent people who understand the psychology of various, age, sex and occupational groups. In setting their strategies, they manipulate the minds and massage the egos of the most vulnerable group of young adults who are so impressionable. This scenario is exacerbated by the undue emphasis on wealth and material possession by the Nigerian society where the end seems to justify the means.

Rather than resort to the "fire brigade" approach to crime control that has become the norm rather the exception in Nigeria, the government should dedicate more energy and resources in addressing the social conditions that give rise to cyber crime. The various efforts by law enforcement agencies to combat the menace of cyber crime will only be successful and sustainable if the real victims and targets are made less suitable for on-line victimization.

Anti-cyber crime campaigns should be taken to post-primary schools and institutions of higher learning. The virtues of honesty, hard work and integrity should be taught our youths. Every effort should be made to practically demonstrate to the youth of this generation and the upcoming ones that there is dignity in labor and that work is gain not pain. Also more recreational facilities should be provided in schools and cities across Nigeria. They should be properly secured from touts and street urchins and made accessible to adult Nigerians and accompanied minors free of charge. The Nigerian society needs to redefine where it stands on the issue of wealth acquisition. Rather than celebrate wealth per se, she should celebrate service and dignity. This is one way of saving internet active Nigerians from the pains of cyber crime victimization.

References

Adeniran, A. I. (2008). The Internet and Emergence of Yahoo-boys sub-Culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368–381.

Adeniran, A. (2011). Café culture and heresy of yahooboyism in Nigeria. In K. Jaishankar, (Ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. 3-12). Boca Raton, FL, USA: CRC Press.

Agbefu, R. E., Hori, Y., & Sakurai, K. (2013). Domain information blacklisting method for the detection of malicious webpages. *International Journal of Cyber Security and Digital Forensic*, *2*(2), 36 -47.

Alshalan, A. (2005, September, 21). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*. Published by Department of Sociology, Anthropology, and Social Work, Mississippi State University. Retrieved on 15th August 2013 from http://www.cse.msstate.edu/~dampier/study%20materials/NationalCrimeStats.pdf

Ayofe, A. N., & Oluwaseyifunmitan, O. (2009). Towards ameliorating cyber crime and cyber security. *International Journal of Computer Science and Information Security*, *3*, 1-11.

Bossler, A. M., & Holt, T. J. (2010). The Effect of self-control on victimization in the Cyberworld. *Journal of Criminal Justice, 38,* 227-236.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber crime. *Policing: An International Journal of Police Strategies and Management*, *29*(2) 408 – 433.

Choi, K. (2006). An empirical assessment of an integrated theory of cyber-crime victimization. Paper presented at the annual meeting of the American Society of Criminology (ASC), Los Angeles, CA, USA.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical Assessment. *International Journal of Cyber Criminology, 2*(1) 308-33.

Clarke, R., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to do about It*. New York: Harper Collins Publishers.

DeBell, M., & Chapman, C. (2003). *Computer and Internet use by children and adolescents in the United States,* 2001 (NCES 2004-014). U.S. Department of Education. Washington, DC: National Center for Education Statistics, 2003.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19,* 468-83.

Fox, K. A., Nobels, M. R., & Piquero, A. R. (2009). Gender, crime, victimization and fear of crime. *Security Journal*, *22*, 24-39.

Frate, A. A. D. (2003). The voice of victims of crime: Estimating the true level of conventional crime. *Forum of Crime and Society*, *3*(1), 127 – 140.

Halder, D., & Jaishankar, K. (2010). Cyber Victimization in India: A Baseline Survey Report. Tirunelveli, India: Centre for Cyber Victim Counseling. Retrieved on 15th August 2013 from http://www.cybervictims.org/CCVCresearchreport2010.pdf

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30,* 1-25.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470 – 486.

Livingstone, S., & Helsper, E. (2007). Taking risks when communicating on the internet: the role of offline social-psychological factors in young people's vulnerability to online risks. *Information, Communication and Society, 10,* 619-643.

Longe, O. B., & Chiemeke, S. C. (2008). Cyber crime and Criminality in Nigeria – What Roles are Internet Access Points Playing? *European Journal of Social Sciences, 6*(4), 132-139.

Lusthans, J. (2013). How organized is organized cyber crime? *Global Crime, 14*(1), 52 – 60.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology, 2,* 346-367.

McQuade, S. C. (2006). *Understanding and managing cyber crime.* Boston: Pearson/Allyn and Bacon.

National White Collar Crime Centre and the Federal Bureau of Investigation, (2010). Internet Crime Compliant Centre - IC3, Internet Crime Report. January 1, 2009 – December 31, 2009. Retrieved on 15th August 2013 from http://www.ic3.gov/media/annualreports.aspx

Ngo, F. T., & Paternoster, R. (2011). Cyber crime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5,* 773 – 793.

Odapu, S. M. (2008, September, 15). Nigeria: EFCC develops software to combat cyber crime. *All Africa News,* Retrieved on 15th August 2013 from http://allafrica.com/stories/200809161127.html

Ojedokun, U. A., & Eraye M. C. (2012). Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. *International Journal of Cyber Criminology, 6*(2), 1001–1013.

Ribadu, N. (2007). A welcome address presented at the West African sub-regional meeting on advance fee fraud jointly organized with INTERPOL at the EFCC Training and Research Institute (TRI) Karu, Abuja. *Current Trends in Advanced Fee Fraud in West Africa,* Retrieved on 15th August 2013 from www.efccnigeria.org/index. php?option=com_docman&task= doc_ download&gid=9

Sharma, R. (2007). Peeping into a hacker's mind. Can criminological theories explain hacking? *Social Science Research Network.* Retrieved on 15th August 2013 from http://ssrn.com/abstract=1000446

Stolzenberg, L., & D'Alesso, S. (2008). Co-offending and the age-crime. *Journal of Research in Crime and Delinquency, 45(1),* 65-86.

Tade O., & Aliyu, I. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria *International Journal of Cyber Criminology, 5*(2), 860–875.

Wada, F., & Odulaja, G. O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICT, 5,* 69-82.