PREVALENCE OF CYBERCRIMES AMONG YOUTHS IN ONITSHA SOUTH LOCAL GOVERNMENT AREA OF ANANMBRA STATE, NIGERIA

Udelue, Michael Chinonso[1]
udeluechinonso@gmail.com

&

Dr. Bentina Mathias[2]
Mb.alawari@unizik.edu.ng

[1,2]Department of Sociology/Anthropology
Nnamdi Azikiwe University, Awka

Abstract

This study investigated the prevalence of cybercrime among youths in Onitsha South Local Government Area (LGA), Anambra State, Nigeria. The Social Strain Theory (SST) was adopted as the theoretical framework for the study. The study used the mixed-research design. The multi-stage sampling procedurewas used in the selection of 522 adults aged 18 years and above within the study area as study particpants. A researcher-developed questionnaire was used to collect the quantitative data; while the qualitative data were collected using In-Depth Interviews (IDI) guide. The quantitative data collected were processed using the Statistical Package for Social Sciences (SPSS) software and data analysis was performed using descriptive statistics. Two hypotheses stated were tested at 0.05 significant levels using the chi-square (χ^2) inferential statistics. On the other hand, the qualitative data collected were analysed using the manual content analysis. Findings of the study revealed that cybercrime was prevalent among the youths in Onitsha South L.G.A of Anambra State. Hacking, advance fee fraud, identity theft and cyber terrorism were the most prevalent forms of cybercrimes among the youths in the area. Consequently, it was recommended that programmes that can enable the youths achieve useful skills for self-employment should be initiated by the government.

Keywords Prevalence, cybercrime, youths, advance fee fraud,password sniffing

Introduction

The rapid growth of the internet in the 21st century across the globe has had tremendous changes in virtually every institution within different societies. These changes can however, be described in both positive and negative dimensions. Although the positive dimension of internet revolution are fascinating, the negative dimensions are however overwhelming and often produces maladies that often threaten the social order of the society (Ibikunle & Eweniyi, 2013; Odumesi, 2014; Okeshola & Adeta, 2013). One of the negative outcomes of internet revolution across nations, especially in developing nations like Nigeria, is the growing prevalence of cybercrimes. In the view of Odumesi (2014) the rise in technology and online communications has not only produced a dramatic increase in the incidence of cybercrimes but has also resulted in the emergence of what appears to be a new variety of criminal activities.

Cybercrime according to Das and Nayak (2013) is a crime committed mostly by the individuals or organised groups; in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. Cybercrimes also entails offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (Chat rooms, emails, etc) and mobile phones (Muraina & Muraina, 2015). Examples of cyber-crime as contained in the work of Kshetri (2010) include: denial of service attacks, cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, ID fraud, cyber terrorism, and cyber extortions.

Cybercrimes are not entirely new with its widespread; nor peculiar to developing nations like Nigeria. For instance, the first highly publicized cybercrimes occurred in November, 1988 in the United States (U.S.), when a 23-year old student, Robert Morris, launched a virus ("Morris Worm") on the internet. Over 6,000 computers of the estimated 60,000 systems linked to the Internet at that time were infected and cost about $100 million to repair the infected systems. As a consequence, Morris got a sentence of 3 years' probation and a $10,000 fine (Stambaugh, Beaupre, Icove, Baker, Cassaday & William, 2001). Subsequently, cybercrime gradually evolved into serious global problem. For instance, in 2008, companies worldwide lost more than $1 trillion on intellectual property due to data theft and cybercrime (McAfee, 2009). According to the 2009 World Internet Crime Report released by the Internet Crime Complaint Centre (ICC) (2010), internet-related criminal activities resulted in the loss of about $559.7 million, showing a significant increase from $264.6 million and $239.1 million reported losses in 2008 and 2007 respectively.

Meanwhile, a majority of the 146,663 cases referred for investigation in the US by IC3 involved alleged fraud had a median financial loss of $575 million. Again, there is an increase from $264.6 million in 2008.

It is worthy of note that cybercrime is associated with age. In other words, youths are mostly involved in cybercrimes and as such, the problem is more prevalent in developing nations like Nigeria. Within the ambit of extant literatures, several factors are perceived as being associated with youths' engagement in cybercrime. For instance, Ndubueze, Igbo and Okoye (2011) noted that cyber criminals are mostly people between the ages of 20-35 years. Okeshola and Adeta (2013) also asserted that cyber-crime is often more prevalent among youths who are males. To buttress this, Internet Crime Complaint Centre (ICC) (2010) reported that greater percent of perpetrators of cybercrime were predominantly males. Other studies have pointed towards other factors such as exposure or access to computer/internet facilities, quest for quick wealth, unemployment, lack of implementation of cyber-crime laws, inadequately equipped law enforcement agencies, negative role models, quest for socio-political recognition/fame, frustration, display of wealth by corrupt politicians and laziness, among other factors (Longe & Chiemeke, 2008; Okeshola & Adeta, 2013).

Be that as it may, crimes vary significantly from society to society. As such, one cannot conclude in a hurry that crimes such as cybercrime are prevalent in every society. This is in consideration of the fact that as much as the researcher knows, researches prevalence of cybercrime within the context of Onitsha South L.G.A has been relatively scarce. Hence, there is a gap in knowledge on theme of this study within the context of this present study area. It is against this backdrop that this study is positioned to examine prevalence of cybercrimes among the youths in Onitsha South L.G.A of Anambra State, Nigeria.

The Problem

Computer applications are supposed to be leveraged upon to build the technical knowledge and skills of youths in various industries, Art and commerce; and importantly, in technological advancement. However, reverse has been the case with the Nigerian situation. It has been established by previous studies that cybercrimes among the youths have become very prevalent in many parts of Nigeria (Oluwadare, Oluwasnmi & Igbekoyi, 2018); and occurs in daily bases.

The problem has often attracted the attention of the government, religious institutions and other concerned security agencies into devising measures and policies that could ameliorate this trend. For instance, the Cybercrime Act (2015) makes the provision that any individual or group of individuals found guilty of hacking or unlawful accessing of a computer system or network, are liable to a fine of up to ten million (N10 million) naira or a term of imprisonment of 5 years (depending on the purpose of the hack). Yet, the trend of cybercrime has seen a dramatic influx of many vibrant youths into more dynamic forms of cybercrimes and this poses a huge burden on the general society. Its effects on the reputation of the country and on the physical and mental well-being of victims cannot be overemphasised.

The problems noted above may not be far-fetched within the context of Onitsha South L.G.A, being one of the popular commercial zones in the Southeast Nigeria with a lot of youths hustling day after day to make ends meet. It is also feared that with the alarming popularity of the cybercrime business and its flourishing nature within the Nigerian context, more youths would join in the act, which would worsen the situation and invariably produces a more adverse effects on the sustainability of the Nigerian economy, as well as the usefulness of the youths towards socio-economic growth. Thus, it is envisaged in this study that a way of averting this ugly trend is to scientifically examine public perception about the trend particularly within Onitsha South L.G.A. This is considering the fact that serious research efforts as much as the researcher knows, have not been focused on this area of research interest, particularly within the context of Onitsha South L.G.A. It is therefore, against this backdrop that this study is positioned to investigate the prevalence of cybercrimes among youths in Onitsha South L.G.A of Anambra State, Nigeria.

Objectives of the Study

The study aimed to achieve the following objectives:

1. To determine the prevalence of cybercrimes among youths in Onitsha South L.G.A of Anambra State.
2. To identify the forms of cybercrimes that prevails among the youth in Onitsha South L.G.A of Anambra State.
3. To explore effective measures that could reduce the trend of cybercrimes among the youth in Onitsha South L.G.A of Anambra State.

Study Hypotheses

The following hypotheses were tested at 0.05 significant levels.

1. Female respondents are more likely to perceive cybercrime among the youth as a prevalent phenomenon in Onitsha South L.G.A than their male counterparts.

2. Respondents with higher educational attainment are more likely to identify the prevailing forms of cybercrimes among the youth in Onitsha L.G.A of Anambra State, than those with relatively lower educational attainment.

Brief Review of Relevant Literatur

Concept of cybercrime According to Maitanmi (2013) cybercrime is a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Similarly, Okeshola (2013) opined that the term cybercrime can be used to describe any criminal activity which involves the use of computer or the internet network, including such crimes as fraud, theft, blackmail, forgery, and embezzlement. These two definitions are very narrow in the sense that it does not give a holistic view about what cybercrime is all about. As a consequence, the European Commission as cited in Nigerian Communications Commission ('n.d') noted that a threefold definition for cybercrime is: 1) traditional forms of crime such as fraud or forgery, though committed over electronic communication networks and information systems; 2) the publication of illegal content over electronic media (e.g. child sexual abuse material or incitement to racial hatred); 3) crimes unique to electronic networks, e.g. attacks against information systems, denial of service and hacking.

Furthermore, the Home Office and the SOCA-led Cyber Threat Reduction Board (TRB) as cited in House of Common (2013) defined cybercrime by using a three-fold categorization including:

i. Pure online crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to enable further crime);

ii. Existing crimes that have been transformed in scale or form by use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale; and

iii. Use of the internet to facilitate drug dealing, people smuggling and many other 'traditional' types of crime.

This definition seems more comprehensive because it covers comprehensive aspects that could be associated with crimes using internet facilities. Based on the above conceptualisations, cybercrimes in this study is defined as any criminal act relating to the use of electronic means with the sole aim of gaining financial or other personal benefits at the detriment of other people.

Forms of Cybercrimes There are several types of cyber-crimes some of which explored in this section.

a) Cyber terrorism: A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Matusitz (2005) a cyber-terrorist is someone who intimidates a government or to advance his or her political or social objectives by launching computer-based attack against computers, network, and the information stored on them. In this view, Olusola, Samson, Semiu and Yinka (2013) defined cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. It means that any act intended to instil fear by accessing and distorting any useful information in organizations or government bodies using computer and internet is generally referred to as cyber terrorism. Another form of cyber terrorism is cyber extortion and it is a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service (Hassan, Lass & Makinde, 2012).

b) Fraud - Identity theft: Fraud is a criminal activity in which someone pretends to be another person and retrieves vital information about the person; for instance, making a false bank webpage to retrieve information of someone's account. The concept is simple and simply connotes someone gaining access to another' personal information and uses it for his or her own benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to ATM and using such people can make themselves a lot of money with personal information. In Nigeria people design web links forms requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes (Olusola, Samson, Semiu &Yinka, 2013).

c) Drug trafficking deals: Another type of cyber-crime is drug trafficking; according to Hassan, Lass and Makinde (2012), it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other internet technology. Some drug traffickers arrange deals at internet cafes, use courier web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs (Nosrati, Hariri & Shakarbeygi, 2013).

d) Malware: Malware refers to viruses, Trojans, worms and other software that gets onto your computer without you being aware it's there. Back in the early part of the century, most such software's primary aim was thrill. The people writing the software found it amusing to write a program that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more dangerous. In some cases, a piece of malware will pretend to be a legitimate piece of software. When such software is downloaded, it infects the computer system and destroys valuable information. The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The stolen assets are removed one slice at a time (Olusola, Samson, Semiu &Yinka 2013).

e) Cyber stalking: Cyber stalking is essentially using the internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. People leave a lot of information about themselves online (Acquisti & Gross, 2009). Such information can leave one vulnerable to cyber stalking, a term that essentially refers to using the internet to stalk (to illegally follow and watch somebody) (Lewis, Kaufman & Christakisin, 2005). Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties (Nosrati, Hariri & Shakarbeygi, 2013).

f) Spam: this is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam etc. Some of these address harvesting approaches rely on users not reading the fine print of agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site (Saul, 2007). Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. This is because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer (Hassan, Lass & Makinde, 2012).

g) Logic Bombs: A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display “I gotcha” on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times (Olusola, Samson, Semiu & Yinka 2013). Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn’t find the employee’s name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes (Hassan, Lass & Makinde, 2012).

h) Password Sniffing: Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user name and a password as required when using certain common internet services like file transfer protocol (FTP) (which is used to transfer files from one machine to another) or Telnet (which lets the user log in remotely to another machine) the sniffer collects that information (Peter, Kenneth, Lucasz, Tom & Michael, 2006).

Theoretical Framework

The Social Strain Theory (SST) was adopted as the theoretical framework for this study. It was developed within the socio-structural context of the United States by Merton (1938). The major tenet of this theory lies on the postulation that when opportunities for achieving the socially desirable goals are blocked, those affected may react in react in different ways to adapt to their situation. To him, there are five distinct ways through which people can adapt to social strain including: i) conformity; ii) innovation; iii) ritualism; iv) retreatism and; v) rebellion.

Among these classifications, innovation is of major interest to drive the point with regards to the issue of cybercrime in this study. In this direction, innovation is the ability to develop new means of achieving socially desired ends. As such, innovators aim at fulfilling the goals of the society but instead using legitimate channels, they find other means to reach their goals. In other words, when the legitimate channels of achieving socially desirable goals are perceived as being too stringent by some people, they become innovative in finding ways of meeting such goals using other means. Cybercrime is one of the innovative means adopted by a number of youths in Nigeria to amass wealth, considering the view that other criminal acts such as armed robbery and kidnapping etc; are perceived as becoming more riskier for them due to improved security networks past few years. Thus, youths' involvement into cybercrime is a rational calculation that such crime within the Nigerian context is less risky and can attract wealth within one's private environment.

This theory is also important for this study considering the fact it could help to provide the reason why cybercrimes may be prevalent within the context of the present study area; by pointing towards the social strain experienced by many youths in Nigeria, which is a major push factor to crimes, especially cybercrimes. It is in view of the above backdrop that this theory was chosen as the theoretical framework for this study.

Materials and Methods

This study employed the mixed research design. The area of the study was Onitsha South L.G.A of Anambra State. The population of this study area according to the National

Population Commission (2006) was 137,191. This figure was projected to the date of this present study (i.e. 2019), to give projected population of 208,530. However, the target population for the study included the adult residents of Onitsha South L.G.A who were 18 years and above. According to the National Bureau of Statistics (2010), the proportion ratio for this population category in all L.G.As within Anambra State is 56.1% of the entire population. In this view, the target population for this study is put at 116,985 (i.e. 56.1% of the population of Onitsha South L.G.A).

The sample size was Five hundred and twenty-two (522) adult residents of Fegge-Onitsha South LGA. The sample size for this study was determined statistically using the Cochran (1963) formula for infinite (indefinite) population. The formula is $n = \frac{Z^2(pq)}{e^2}$

Where:

n = required sample size

z = level of significance (95% or 1.96)

p = the proportion of residents of Onitsha South LGA 18 years and above in the total population of residents of Onitsha South LGA is 68% or 0.68%

q = complement of p will be 0.32%

e = accuracy level or error margin (4.0%)

Applying the formula

$$n = \frac{1.96^2(0.68)(0.32)}{0.04^2}$$

$$n = \frac{3.8416(0.68*0.32)}{0.0016}$$

$$n = \frac{0.8359}{0.0016}$$

$$n = 522$$

This study adopted a multi-stage sampling procedure. First, the study used the political ward arrangement in clustering the various areas within the study area. Secondly, the various streets within each of the political wards were identified and using the simple random sampling technique, one street was selected from each of the political wards. These gave a total of 17 streets. In each of the selected streets, the houses contained therein were arranged according to their street numbers and 31 houses were selected using the systematic sampling technique with a random start. This gave a total of five hundred and twenty-seven (527) households. Furthermore, in each of the selected households, one eligible respondent was selected using the purposive or availability sampling as the case maybe, based on the criteria of age (18 years and above). In situations where an eligible respondent was not available with a selected household, such households were skipped to the next available one and this process was repeated where applicable until the target was achieved. On the other hand, the purposive sampling technique was used to select relevant individuals who participate in the In-Depth Interview.

The mixed approach was applied in the instruments used for data collection. This involved the use of a researcher-developed questionnaire to collect the quantitative data; and In-Depth Interview (IDI) to collect the qualitative data. Data were collected from the sampled respondents on face-to-face basis by the researcher and paid research assistants. Out of the 522 copies of the questionnaire distributed, only 510 copies (representing 97.7% of distributed questionnaire copies) were usable for data analysis. Quantitative data collected were processed using the Statistical Package for Social Sciences (SPSS) software, while data analysis was conducted using frequency counts, and simple percentages. The study hypotheses were also tested using the chi-square inferential statistics; while the data generated through qualitative data were transcribed, translated and analysed using manual content analysis.

Research Findings/Results

Table 1: *Composite Analysis of Socio-Demographic Characteristics of the Respondents*

Socio-Demographic Variables	Frequency	Percent
Sex		
Male	303	59.4
Female	207	40.6
Total	510	100.0
Age Category		
18-22 Years	121	23.7
23-27 Years	115	22.5
28-32 Years	123	24.1
33-37 Years	104	20.4
38 Years & above	47	9.0
Total	510	100.0
Marital Status		
Single	310	60.8
Married	187	36.8
Separated/Divorced	10	2.0
Widowed	3	.6
Total	510	100.0
Occupation		
Farmer	7	1,4
Trader	97	19.2
Civil servant	216	42.4
Artisan	22	4.3
Student	131	25.7
Unemployment	8	1.6
Others	29	5.7
Total	510	100.0
Level of Educational Attainment		
No formal education	5	1.0
Primary education	8	1.6
Secondary education	179	35.1
Tertiary education	318	62.4
Total	510	100.0
Religious affliction		
Catholic	289	56.7
Protestant	189	37.1
African Traditional Religion	3	.6
Anglican	29	5.7
Others	-	-
Total	510	100.0
Monthly Income		
Less than ₦15,000	54	10.6
₦16,000 – ₦30,000	186	36.5
₦31,000 – ₦45,000	116	22.7
₦46,000 – ₦55,000	54	10.6
₦56,000 – ₦65,000	18	3.5
₦66,000 – ₦75,000	3	0.6
₦76,000 & Above	79	15.5
Total	510	100.0

Field Survey, 2019.

Table 1 show that a majority (59.4%) of the respondents were the males, while 40.6% were females. The age range with the highest frequency is 26-29 years, while the least frequency occurred within the age category of 38 years and above. The age mean of the respondents was 27 years. This suggests that the respondents were adult-youths who are mature enough to provide the need data for this study. The table also shows that a majority (60.8%) were single, while about a quarter (36.8%) of them was married. The data also indicate that 2.0% of the respondents were separated/divorced, while a very lower proportion (0.6%) widowed. Furthermore, it can be deduced from the table that civil servants (42.4%) make the highest respondents in the category of occupation. This was followed by students that accounted for 19.2% in the sample, while traders accounted for 19.0%, and other professions accounted for 5.7%. Artisans accounted for 4.3%, the unemployed were 1.6% of the sample, while the least in the population were farmers – accounting for 1.4% of the sample.

With respect to the respondents' level of educational attainment, the data show that a majority (62.4%) attained up to tertiary level of education. This is followed by 35.1% who only attained up to the secondary school level. 1.6% of the respondents only attained the primary school level; while a very lower proportion (1.0%) of them indicated that they had no formal education. This implies that majority of the respondents are educated and could read and respond to the questionnaire. Furthermore, the table revealed that majority of the respondents who were Catholics accounted for 56.7%. This is followed by the Protestants which were 37.1% of the respondents, while the Anglicans were 5.7% and the least with 0.6% were those of the African Traditional Religion accounted for .6%. Interestingly, none indicated to be of other faiths, like Islam. This may not be strange since the study was carried out in Onitsha South which is predominantly inhabited by good number of Christians. Lastly, a majority (36.5%) indicated that they earned a monthly income within the range of ₦16,000.00 – ₦30,000.00; while the least proportion (0.6%) of them earned within a monthly income of ₦66,000.00 – ₦75,000.00. On the average a good number of the respondents earn about ₦50, 940.00 per month. This suggest that majority of the respondents were middle income earners.

Analysis of Research Objective 1 The researcher was interested in determining the prevalence of cybercrimes among the youths in the study area. This was ascertained through the opinion of members of the public sampled for this study. Analysis of findings with regard to this is presented in table 2.

Table 2: *Respondents Views on Prevalence of Cybercrime in Onitsha South*

Items Description	Options	Frequency	Percent
Respondents' Views about Prevalence of Cybercrime	Yes	483	94.7
	No	19	3.7
	Not Sure	8	1.7
	Total	**510**	**100.0**
Perception of youths a being involved in cybercrime	Yes	504	98.8
	No	6	1.2
	Not Sure	-	-
	Total	**510**	**100.0**
Respondents' Ratings about the level of cybercrime among youths.	High	385	76.4
	Moderate	98	19.4
	Low	21	4.2
	Sub-Total	**504**	**98.8**
	Missing Values	6	1.2
	Total	**510**	**100.0**
Respondents' Views on the age bracket mostly involve in cyber-crime in Onitsha South.	18-23 Years	111	21.8
	24-29 Years	241	47.3
	30-35 Years	52	10.2
	36-41 Years	22	4.3
	42 Years & Above	84	16.5
	Total	**510**	**100.0**

Field Survey, 2019.

Note: *Missing values represent some of the items which the respondents skipped or refused to respond to.*

Table 2 contains items which were designed to measure the prevalence of cybercrime in Onitsha South L.G.A, Anambra State. From the result, a majority (94.7%) of the respondents perceived that cybercrime is prevalent in the study area. A lower proportion (3.7%) of them did not perceive it as such as existing in their areas; while a very lower proportion (1.7%) of them was unsure about it. When asked if they perceive youths in the area to involve in cybercrime, 98.8% of the respondents said 'yes', while only 1.2% of them indicated 'No'. Further probe indicates that out of the 98.8% persons that said youths in the area were involves in cybercrime, a majority (76.4%) of them rated the level of cybercrime among youths in the area to be high, while 19.4% said it was moderate and just 4.2% says it was low. This suggests that cybercrime is widespread among youths in Onitsha South L.G.A. This may be attributed to the attraction and high level of urbanization of the area due to the presence of the Onitsha main market. Lastly, about 47.3% of the respondents indicated that cybercrimes were more prevalent among youths between the ages of 24 to 29. Again, this may be linked to the high level of unemployment in the nation in general and Anambra state in particular; and also considering the fact that this age bracket is usually the period of graduation from higher institutions of learning and stage of settling down to build one's family or business establishments. So the fear of not making it, perhaps due to unemployment and economic hardship could at this stage trigger thoughts of criminalities. These views were supported by an interviewee, who noted that,

> Almost every day you find young men from ages 22-30 years engaging all sort of illegal means of survival. In this area alone there have been reported cases of attempted ritual on old men and women. These young men will kill anyone just to make illegal money through the internet. Not once, not twice have we caught young boys with human parts in the early hours of the day. In our days we wanted genuine money but young boys of nowadays will do anything for quick money (Male, 59 year, Association Chairman, Fegge, Onitsha South L.G.A).

Additionally, another interviewee opined that,

> Well, 'yahoo yahoo' is a now a daily occurrence within this area. You see all these young well everywhere, many of them are soiling their hands into the yahoo yahoo business because everybody wants to make it, to ride big cars, and build big mansions; mainly because in this society, if you have all these, you have security, connection and influence. That is the reason why many of them are joining the crime so as to obtain quite wealth and have influence in the society (Male, 62 Years, Association Chairman, Odoakpu, Onitsha South L.G.A).

It was assumed however, through the study hypotheses that female respondents were more likely to perceive cybercrime among the youth as a prevalent phenomenon in Onitsha South L.G.A than their male counterparts. To test this hypothesis, the chi-square statistical tool was employed. Results of the test are shown in table 3.

Table 3: *Summary of Chi-Square Test Between Gender and Perception about Prevalence of Cybercrimes among Youths.*

Perception about Cybercrime among Youths	Respondents' Gender		Total
	Male	Female	
Prevalent	300(61.1%)	191(38.9%)	491(100.0%)
Not Prevalent	13(68.4%)	6(31.6)	19(100.0%)
Total	313(61.4%)	197(38.6%)	510(100%)

Pearson Chi-Square χ^2 = 3.841, *df* = 1, *N* = 510, *p* = .637

The chi-square statistical test was run to test if the respondents' perception about the prevalence of cybercrimes among the youths is associated with their gender. Consequently, the result of the test shows a statistically significant evidence to reject the stated alternate hypothesis, (H_1), (χ^2 = 3.841), *df* = 1; *p* = .637. This implies that the both male and female respondents had similar views about the prevalence of youth involvement in cybercrimes in Onitsha South L.G.A.

Analysis of Research Question 2 Thhe second objective of this study was to determine the most prevailing forms of cybercrimes in the study area. Consequently, the respondents were asked to indicate the major forms of cybercrimes which the youth in Onitsha South L.G.A mostly engage into. The findings are presented in table 4.

Table 4: *Respondents Views on forms of Cybercrime existing in Onitsha South*

Forms of Cybercrime	Responses		Percent of Cases
	N	Percent	
Cyber terrorism	78	10.9%	49.4%
Identity theft	145	20.2%	91.8%
Drug trafficking deals	51	7.1%	32.3%
Malware	24	3.3%	15.2%
Cyber stalking	59	8.2%	37.3%
Hacking/Spam	114	15.9%	72.2%
Logic bombs	13	1.8%	8.2%
Password sniffing	76	10.6%	48.1%
Advance-fee-fraud	158	22.0%	100.0%
Total	**718**	**100.0%**	**454.4%**

a. Dichotomy group tabulated at value 1.

Field Survey, 2019.

In table 3, the Multiple Response Data Set (MRDS) was used to determine the existing forms of cybercrimes in Onitsha South L.G.A, within the knowledge of the respondents.

This statistical tool was employed due to the fact that the question presented to the respondents was in multiple options/response formats. This means that the respondents answered either 'Yes' or 'No' in each of the given items – 'Yes' in any of the items signified that a respondent agreed that such form of cybercrime existed, while 'No' signified that such form of cybercrime does not exist. In all, the MRDS was used to calculate the valid responses for each case to obtain the overall percentage of responses. Consequently, the result of the analysis shows that a majority (22.0%) of the respondents indicated that advanced fee fraud was the most prevailing form of cybercrime in Onitsha South L.G.A. This is followed by 20.2% of the respondents who affirmed that identity theft was the major prevailing form of cyber crime. Other prevailing forms of cybercrime according to degree of agreement by the respondents include: Hacking/Spam (15.9%), Password sniffing (10.6%), Cyber stalking (8.2%), drug trafficking deals (7.1%), Malware (3.3%) and Logic bombs (1.8%).

Data from an In-depth interview conducted with a 52 years old woman leader support the above findings. According to her

> There are various types of cybercrime existing in this area. Daily we hear of and observe cybercrimes such as: hacking, yahoo business, internet scamming, ID fraud, Automated Teller Machine fraud, uploading and watching pornography and other minor cases that I can't even recall their names (Female, 52 Years, Women Leader, Fegge, Onitsha South L.G.A).

This view was also supported by another respondent who was of the opinion that,

> Hacking of people's accounts is very rampant in this area. You know, these yahoo yahoo guys are really organising themselves and learning from each other the easiest patterns to defraud people. So, they can hack one's account without any security alert. The only thing you will see is that all your savings have been stolen. Other types we mostly experience here are identity theft, online job deals and spams (Male, 50 Years, Civil Servant, Odoakpu, Onitsha South L.G.A).

In this study, the researcher assumed that respondents with higher educational attainment were more likely to identify the prevailing forms of cybercrimes among the youth in Onitsha L.G.A of Anambra State, than those with relatively lower educational attainment. To test this assumption, the chi-square test was also used and the result of the test is shown in table 5.

Table 5: *Summary of Chi-Square Test Between Respondents' Level of Educational Attainment and their Views about Cybercrime as being Dangerous.*

Knowledge of Most Prevailing Forms of Cyber crime	**Respondents' Education Level**		**Total**
	Lower Educated Persons	**Higher Educated Persons**	
Yes	186(36.9%)	318(63.1%)	504(100.0%)
No	6(100.0%)	0(.0%)	6(100.0%)
Total	192(37.6%)	318(62.4%)	510(100%)
Pearson Chi-Square χ^2 = 10.056, *df* = 1, *N* = 510, *p* = .002			

Respondents' knowledge about the most prevailing forms of cybercrime among youths in the study area was tested based on their level of educational attainment using the chi-square statistical test. The result of the test shows a statistically significant evidence to accept the stated alternate hypothesis, (H_1), (χ^2 = 10.056), *df* = 1; *p* = .002. This infers that higher educated respondents have the more propensities to know the most prevailing forms of cybercrimes among youths than those who have relatively lower levels of educational attainment. This could be that those with higher education have advanced knowledge about cybercrime to academic exposure and research compared to those with lower educational attainment.

Analysis of Research Objective 3 Considering the view that cybercrime is a social menace in the society, the researcher sought to find out measures that could be employed to control the trend of cybercrimes among youths especially within the context of Onitsha South L.G.A. In this direction, the respondents were asked to express their views about how cybercrime among youths in the study area could be curbed. There respondents are presented in table 6.

Table 6: *Respondents' Views on how Cybercrime can be Curbed or reduced in Onitsha South L.G.A*

Options	Frequency	Percent
Provision of Employment Opportunities to the Youth	162	31.8
Enacting and implementing stricter laws against cybercrime	68	13.3
Parental monitoring	20	3.9
Establishment of formidable Internet Security Agency to Detect Cybercrimes	64	12.5
Confiscation of properties belonging to arrested cyber criminals.	110	21.6
5-10 years jail term for cybercriminals	86	16.9
Others	-	-
Total	**510**	**100.0**

Field Survey, 2019.

The data in table 6 revealed that a majority (31.8%) of the respondents suggested that cybercrimes among the youths in Onitsha South L.G.A could be reduced through the provision of employment opportunities to them. This is followed by 21.6% of them who opined that it could be reduced through confiscation of properties belonging to arrested cyber criminal. This could give other cyber criminals the view that once they are caught, all their efforts would be a waste; thus causing them to rethink about the cyber business. Meanwhile, 16.9% opted for the option of 5-10 years jail term for cyber criminals. 13.3% of them were of the view that making and implementing laws against cybercrime would be a sure measure to reduce the problem of cybercrime. Additionally, 12.5% of the respondents had the view that establishment of formidable internet security agency to detect cybercrimes activities would go a long way in reducing the problem of cybercrimes involvement among the youths; while a very lower proportion (3.9%) of them opined that parental monitoring could be a possible measure to curtail the trend of cybercrimes among the youth in Onitsha South L.G.A.

Reacting to this issue through the IDI, an interviewee had the view that,

> If you want to solve a problem, you have to first identify the cause of the problem. For me, I think that the problem associated with increased involvement of youths into cybercrime has to do with first societal placement of values on wealth acquisition and achievement as a measure of social status, without available opportunities for youths to achieve such. Therefore, I feel that once the government decides to make life easier for the populace, especially the youth through provision of enabling environment where those who cannot find cooperate job, could engage themselves in meaningful self-employed jobs, the problem of cybercrime will be reduced (Male, 57 Years, Social Analyst, Fegge, Onitsha South L.G.A).

For another interviewee,

> Any youth caught involving in cyber related crimes should be punished possibly with 10 years jail terms and corresponding imposition of fines. With this, other youths would understand that yahoo yahoo business is a grievous crime. I mean, it will serve deterrence to others intending to join the business. Most importantly, the issue of unemployment has to be practically addressed if not, new patterns of cybercrime will emerge and may be more grievous compared to the existing forms (Female, 53 Years, Civil Servant, Onitsha South L.G.A).

Discussion of Findings

The majority of the respondents perceived cybercrime as being prevalent among the youths within the study area and this trend was most prevalent among youths between the ages of 24 – 29 years. The view about the prevalence of cybercrime among youths in the study area, cut across respondents' gender as indicated by the test of hypothesis regarding the prevalence of cybercrimes in Onitsha South L.G.A, Anambra State. This finding can be tied to the report of National White-Collar Crime Centre (2010) and the Federal Bureau of Investigation (2010) who separately revealed that Nigeria has for four consecutive years (2006, 2007, 2008 and 2009) ranked third on the list of world cybercrime perpetrator countries. These findings are however, in contrast with that of Zayid and Farah (2017) who found that the respondents in their study had low knowledge about the prevalence of cybercrime in Saudi Arabia.

This study also found that among the different forms of cybercrime, hacking, advance fee fraud, identity theft and cyber terrorism were the most prevalent forms of cybercrime in the study area. This finding is in line with Okeshola and Adeta (2013) who found that 'hacking' was on the top list among the various forms of cybercrime found in their study. However, studies such as and Idom and Taomusa (2016) were at variance with the findings of this present study; as they concluded in their study that scams/spam, lotteries fraud and employment fraud were on the top list of the forms of cybercrimes found in their own study.

Measures that could be introduced to curb the trend of cybercrimes among the youth as found through the data analysis in this study include: provision of employment opportunities for the youth, confiscation of properties belonging to arrested cybercriminals, 5-10 years jail term for cybercriminals to serve as deterrent to potential cyber criminals, enactment and implementation of stricter laws against cybercrime and establishment of formidable internet security agency to detect cybercrimes activities and cybercriminals. These suggestions coincide with the submission of Adesina (2017) who recommended that the government need to address the problem of youth unemployment and increasing poverty level which is a push factor towards property and other related crimes in Nigeria.

Conclusion/Recommendations

This study was motivated by the desire to understanding the trending prevalence of cybercrime involvement by the youths in Nigeria which is feared to cross across every major parts of the country, especially in Onitsha South L.G.A. This study envisaged that understanding the prevalence of cybercrimes among the youth from the views of the members of the public would give a clue to understanding the major aspects associated with the issue under discourse. Thus, having explored all aspects of data necessary have a full understanding of the theme of this study, the study concludes that cybercrime is a prevalent social-economic crime within the context of Onitsha South L.G.A, just as it is prevalent in other parts of Nigeria as has been documented in extant literature. Factors associated with the prevalence of youth's involvement in cybercrime could be located within socio-structural configuration of the Nigerian society. As cybercrime is found in this study as a problematic issue in almost all parts of the country, particularly in Onitsha South L.G.A; with its attendant effects on people's livelihood as well as the general society, the findings of this study is considered germane and timely to address the issues before it becomes very devastating. It is therefore in view of the foregoing and areas of gap in this study, that this study recommends the following:

1. Government should liaise with the Ministry of youths and sports in the state to enlighten these youths on the dangers of cybercrime and also to help sensitize other youths who may be pressurized by their peers to get involved in cybercrime.
2. There is a need for the government to utilize the bottom-top approach in establishing a social programme or policy that would target the youth especially in skills acquisition and entrepreneurial development. This would make the youth feel that they are valued and carried along by the government; which will in turn engender their sense of social responsibility.
3. Members of the public should be sensitised and updated on the prevailing forms of cybercrimes so as to become aware of them, in order to escape being victimised by cybercriminals. When a majority of the populace are sensitized about this and take proactive actions, the cybercriminals would become less successful, and this will reduce to attractiveness of the cybercrime business.

References

Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, 13(4), 19-29.

Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences, 106,* 10975-10980.

Cochran, W.G. (1963) *Sampling Techniques*, Wiley, New York.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies, 6*(2), 142-153.

Hassan, A. B., Lass, F. D., & Makinde. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology, 2*(7), 626 – 630.

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) 11-114.

Internet Crime Complaint Center - IC3 (2010).Internet Crime Report. January 1, 2009 – December 31, 2009. National White Collar Crime Centre and the Federal Bureau of Investigation. Retrieved from on 5th August 2018 from *http://www.ic3.gov/media/ annual reports.aspx*

Kshetri, N. (2019). Cybercrime and cyber security in Africa. Journal of Global Information Technology Management, 22(2), 77-81

Lewis, K., Kaufman, J., & Christakisin, N. (2005). The taste for privacy: an analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication, 7*(4), 87 – 94.

Longe, O. B., & Chiemeke, S. (2008). Cybercrime and criminality in Nigeria: What roles are internet access points playing? *European Journal of Social Sciences, 6*(4) 132 – 139.

Matusitz, J. (2005). Cyber terrorism. *American Foreign Policy Interests, 2,* 137–147.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672-682.

Muraina, M. B., & Muraina, K. O. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among university undergraduates in South-western Nigeria. *International Journal of Technology in Teaching and Learning, 11*(1), 50-59.

National Bureau of Statistics (2010).Publication of the details of the breakdown of the national and state provisional totals 2006 census. Retrieved on 10th November, 2018 from *http://www.nigeriastat.gov.ng.*

National Population Commission (2006). The Nigeria population census. Retrieved from *http://www.population.gov.ng/index.php?option=com_content&view=artide&id=89*

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cybercrime victimization among internet active Nigerians: An analysis of socio demographic correlates. *International Journal of Criminal Justice Sciences, 18*(2), 225-234.

Nosrati, M., Hariri, M., & Shakarbeygi, A. (2013). Computers and internet: From a criminological view. *International Journal of Economy, Management and Social Sciences, 2*(4), 104-107.

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116 – 125.

Okeshola F. B., & Adeta A. K, (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research, 3*(9), 98-114.

Olusola, M., Samson, O., Semiu, A & Yinka, A. (2013). Cybercrimes and cyber laws in Nigeria. *The International Journal of Engineering and Science, 2*(4), 19 – 25.

Oluwadare, C. T., Oluwasnmi, L. A., & Igbekoyi, K. E. (2018). Prevalence and forms of cybercrime perpetrated by students in public tertiary institutions in Ekiti State. *International Journal of Economics, Business and Management Research, 2*(4), 568-584.

Peter, C., Kenneth, P., Lucasz, M., Tom, P., & Michael, W. (2006). Spamalot: A toolkit for consuming spammers resources. Proceedings of the 3rd Conference on E-mail and Antispam. Retrieved on 15th September, 2018 from *www.ceas.org.*

Saul, H. (2007). *Social network launches worldwide spam campaign.* New York: New York Times.

Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W., & Williams, W. (2001). Electronic crime needs assessment for state and local law enforcement. Retrieved on September 1, 2018 from *http://www.ojp.usdoj.gov/nij/pubs-sum/186276.htm*