PREVALENCE AND FORMS OF CYBERCRIME PERPETRATED BY STUDENTS IN PUBLIC TERTIARY INSTITUTIONS IN EKITI STATE

Oluwadare, C. T,Oluwasanmi L. A. and Igbekoyi K. E.
Department of Sociology,
Ekiti State University, Ado-Ekiti
+2347061338424

Abstract

Educational system in Nigeria is said to be in a pitiable situation as cybercrime perpetrators increases daily. This is because the menace has continued to hit and bite hard on the livelihood of Nigerians. Today, many Nigeria students lack reading culture as they turn lackadaisical attitude towards academy and the clamour for materialism which makes cybercrime to be prevalent. The study made use of qualitative and quantitative methods in data collection. Three hundred and ninety-two (392) questionnaires were distributed to respondents in three purposive selected tertiary institutions in Equity state and eleven (11) in-depth interviews were granted. The study revealed that cybercrime is prevalence among students as an overwhelming percentage distribution affirms to it. It further shows that reported case of cybercrime is on daily bases. Also, the study revealed the types of cybercrime perpetrated by students to be internet advance fee fraud. Hence, the study recommends that school management should cooperate with the Law Enforcement Agencies in checkmating the prevalence of the menace among students of the tertiary institutions. Also, there should be adequate technological training for law enforcement agents in forensic department as this will allow more proactive approach to the Law Enforcement Agencies.

Keywords: prevalence of cybercrime, forms of cybercrime, cyber realm, students, tertiary institutions

Introduction

Introduce the Problem

Curbing cybercrime has remained a difficult task for the law enforcement agencies in Nigeria due to the complex nature in detecting and preventing crime within the cyber space. However, Nigeria law enforcement agencies tend to be limited in operating within a specified jurisdiction in terms of controlling cybercrime and as a result, become necessary to study the prevalence and forms of cybercrime perpetrated by students in public tertiary institutions in Equity state. Basil (2016) posited that there is no agency saddled with the enforcement of the cybercrime Act and no agency truly sees it as their onus. However, the study examined the prospects of establishing some level of control within the cyber realm as suspected cyber fraudsters cannot be effectively controlled due to the nature of monitoring and enforcement within the cyber realm.

Cybercrime has become a social problem since 1980s, and has grown worldwide within the prospect of corrupt activities dealing in foreign exchange and transfer of all illegal money obtained through foreign businesses and enterprises (Gnosis, 2009). Studies on cybercrime focus on the emergence of cybercrime in Nigeria; the perception of cybercrime among Nigeria youths, the nature, causes and consequences of cybercrime in tertiary institution, the extent of involvement in cybercrime activities among students in tertiary institutions, fighting cybercrime in Nigeria and so on. Nevertheless, the growth and development of information and communication technology (ICT) in Nigeria has brought with it great changes in the socio-economic growth and development in different facets of Nigerian economy. At the same time, information communication technology (ICT) has also developed to become an advanced tool in the hands of criminals for perpetrating different forms of crime within the cyber realm (Martins, 2016).

The youth in every society is of great importance and concern to the society because they are regarded as the future leaders (Okesola and Abimbola, 2013). Olive and Adware (2004) observed that a sizeable number of criminals in Nigeria fall within the youthful age. The youths at present have ascertained many ways of using the internet in perpetrating different forms of criminal behaviours and these age groups are usually found in tertiary institutions in Nigeria. However, young students in tertiary institutions engaged in various forms of crimes including examination malpractice, false admission and school fee receipts, rape, robbery & stealing, sexual abuse, cultism and among other. Today, cybercrime has developed into a new form of crime and also exist in Nigeria tertiary institutions which are now denting and drilling holes in the economy of the nation (Domes, 2014).

Nevertheless, the above statement explains how worrisome cybercrime is and how it has become a terrifying situation for law enforcement agencies to control its prevalence among students in tertiary institutions in Nigeria. While the escalation of cybercrime among students in tertiary institutions could not be curtailed adequately by law enforcement agencies, the menace become prevalence and the effects continue to hit and bite hard on Nigeria economy, both locally and internationally. On this premises, the study intends to investigate the prevalence and types of cybercrime perpetrated by students in public tertiary institutions in Equity State.

Objective of the Study

The objectives for the study include the followings;

(i) Examining the prevalence of cybercrime among students in public tertiary institutions in Equity State.

(ii) Identifying the forms of cybercrime perpetrated by students in public tertiary institutions in Equity State.

Relevant Literature Review

Prevalence of Cybercrime in Nigeria

At the turn of 21st century, Nigerian internet infiltration levels have increased rapidly. According to Bengal, Babatope & Bankable, (2012) the number used to be less than 5% in 2002-2003, and later stood at over 30% by the end of 2012 and this growth is only equanimous to speed up. The introduction of mobile telephone on the Nigerian market played a crucial role and a key drive of advancement. At the end of the first quarter of 2016 (January-March 2016), Nigeria is the 16thhighest ranked country moving up two places from 18th position in the previous quarter. Developing nations especially the Africans countries were highly represented in the upper rankings and Nigeria was surpassed by a handful of other African countries, including Namibia and Malawi in second and fourth spots respectively (The news, 2016). However, the rise of the internet in Nigeria has come with a non-deliberated consequence and global notoriety becomes a safe haven for cyber fraudsters. Back in the 90s, fraud in Nigeria society was popular called 419 in reference to section 1(3) of the advance fee fraud and other related offenses Act No. 14 of 2006 penal code that framed the criminal justice system in Nigeria. At the time, person(s) who were arrested in connection to that law were labelled '419ers' (Bengal, et al 2012).

Consumer Reports State of the Net (2007) shows that more than $7 billion cost of cybercrime on U.S consumers was estimated and also, The Internet Crime Compliant Centre (2012), reported that victims had losses over $500,000. In 2012, the Internet Crime Complaint Centre (IC3) received 289,874 consumer complaints, with losses of $525,441,110 (Ndubueze, 2013). According to Ndubueze (2013) it shows 8.3% increase in losses from the previous year and the most affected victim complaint country was the United States with 91.2%. The most frequently reported cybercrimes complaints were auto fraud, military impersonation e-mail scam, romance scam, intimidation/exploitation scam and among others as stressed by Ndubueze, (2013).

To appraise the prevalence of cybercrime in Nigeria, quantitative research was employed in collecting information around losses in terms of money, time and material incurred by citizens through cybercrime. According to Bengal et al, (2012), the prevalence appraisal a survey was used to estimate how many of Nigerian's 48.3 million internet users experienced the loss. This was used to compute the estimated loss for Nigeria. This led to the estimated Nigerian consumer loss of #2,146,666,345,014.75 ($13,547,910,034.80) to cybercrime in 2012 (Bengal, et al 2012). The reported case ranges from fake lotteries to the biggest internet scams. In July 2001, The Economic and Financial Crime Commission (EFCC) arrested four Nigerians suspected to be involved in cybercrime that duped unsuspecting foreign investors in Ghana. Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under false claim. They were arrested at the point of delivery by government officials. Recently, the Ibadan tonal office of the Economic and Financial Crime Commission (EFCC) arrested a 26 year old student of Equity State University, Ado-Equity for internet fraud, deceiving unsuspecting victims on military dating sites posing as Nigeria-based US Army officer by the name Sergeant Frank McGhee (EFCC, 2016).

Types and Practice of Cybercrime

Cybercrime in Nigeria seems to follow a pattern of technology use that is highly advanced. Most of the cybercrime activity took the form of emails scam, where the scammer(s) mail a letter via e-mail and with a scheme to extort money. There can be several types of internet based Advanced Fee Fraud, which include; Transfer of money from over invoiced contracts, Contract Fraud (delivery of goods and service), Conversion of Hard Currency, Sales of Crude oil at below market price, Purchase of Real Estate, Disbursement of money from Wills, Threat Scam and Clearing House just to name a few (Yesinia, 2015). Some of the types and practice of cybercrime perpetrated especially among students in tertiary institutions in Nigeria are stated below as envisaged by Martins (2016).

(1) E-mail scam and spam. Cyber fraudsters' uses these patterns to solicit and present false investment to their unsuspected victims. Locally and internationally, Nigeria's image has been seriously dented by the above schemes of cybercrime such that there is a type of e-mail scam code named the 'Nigerian' E-mail scam. This e-mail scams according to Martins (2016) may come in any of the following ways below;

(a) The cyber fraudster sends an e-mail that the victim is the named beneficiary in the will of an estranged relative and that he/she stands to benefit and inherit an estate worth millions.

(b) Online charity: here the fraudster sends e-mails to their victims soliciting for funds and assistance to charitable organization that do not exist. Such scam contains emotional and touching messages aimed at appealing to the conscience of their victims.

(2) Cyber stalking: there is no universally accepted definition of cyber stalking as posited by Martin (2016). It is generally considered as the use of internet, e-mail or other electronic communication devices to harass a person(s) and thereby causing an injury or damages to the victim.

(3) Hacking: according to Martins (2016), this is a form of cybercrimes which include illegal access, hijacking, bombing, denial of service attack, eavesdropping etc. Some internet users assumed that hacking is harmless, fun and even quite clever, but it can be a serious invasion of privacy and a significant threat to e-commerce.

(4) ATM Fraud: this type of fraud is perpetrated through the ATM machines and e-transaction system. In some cases, the criminals set up their own ATM machines in which the criminal steal the PIN of the users or their cards and use it to withdraw all the money in the victim's account (Martins, 2016).

(5) Illegal e-lotteries: the effort to get rich quickly by most Nigerians especially the youth is often exploited by cyber fraudsters who send all kinds of tempting messages of an existing lottery bonanza where participants can be deceive with all sorts of items and money ranging from cars, electronics, laptops etc. this form of cybercrime is rampant in Nigeria (Martins, 2016). Even the American visa lotteries have been used to lure many Nigerians to their doom as lots of youths are eager to travel abroad and these scammers are aware of this, and they respond by creating online visa lotteries to rip off unsuspecting youths.

(6) Piracy: according to Ovine (2001) he described piracy as the violation of intellectual property. Digital technology makes it very easy to perfectly copy and create products such as music, e-library or films and the internet provides a free and almost anonymous means of transmitting these pirated materials around the world.

(7) Advance fee fraud: this is where Nigerian fraudsters obtain money fraudulently from some foreign nationals, mostly Americans, on the promise of getting married to them or an oil contract. These fraudsters extort money from their victims, promising to be in love with them and agree to marry them and in the process demand for money in which they will use to travel and meet them abroad. Thus, many desperate foreigners seeking for quick means of making money or looking for spouse become victims of these cyber fraudsters (Martins, 2016).

Theoretical Framework

The plausible explanation of cybercrime in the contemporary society as posited by Ovum and Ajani (2013) has always emerged from the synthesis of two or more theories. Therefore, the major theories considered in this work include; Routine Activity and Differential-Association.

Routine activity theory is a crime of opportunity theory that focuses on situations of crimes. It was developed by Marcus Felon and Lawrence Cohen in 1979. This theory attempts to show that crime rates are not generally affected by macro changes such as economic recessions, unemployment rates, poverty etc. This theory stipulates three necessary conditions for most crime; a likely offender (cybercriminals), a suitable target (victims) and the absence of a capable guardian (unprotected information), coming together in time and space. That is, for crime to occur, a likely offender must find a suitable target with the absence of capable guardians. According to Felon and Cohen, (1979), the reason for the increase is that it offers more opportunities for crime to occur, as there is much to steal. Routine activity theory provides a simple and powerful insight into the causes of cybercrime. The idea is that in the absence of effective controls, offenders will prey upon attractive targets. To have a crime, a motivated offender must come to the same place as an attractive target. For property crimes, the target is a thing or an object (usually in cash in the case of cybercriminals) while for personal crimes, the target is a person (wealthy people). If an attractive target is never in the same place as a motivated offender, the target will not be taken, damaged or assaulted. There are controllers whose presence can prevent internet crime such as anti-virus, password or encryption, but if the controllers are absent or present but powerless, cybercrime is possible as posited by Eric (2016).

Differential Association by Sutherland (1960) asserts that an individual is more likely to commit crime when individual learns favourable definition towards violations of the law in excess of the definitions unfavourable to violation of the law. That is, people learning to engage in crime, primarily through their association with others and weighs the benefits between. They learn beliefs that are favourable to crime and as a result, exposed to criminality (McLeod, 2016). Differential Association theory view crime as something that is desirable or at least justifiable in certain situation. It explains both the process by which a given person(s) learns to engage in crime and the content of what is learned. According to Sutherland (1960) an individual's environment influences one to learn appropriate behaviours to survive within the environment. This mostly occurs in group where people within a specific reference group or association display norms of deviance or conformity (Siegel, 2013). According to Siegel (2013), the differential association theory applies to several types of behaviours including cybercrime.

This is because they view themselves as young and innovative; therefore, they commit crimes, such as hacking, advance fee fraud, identity theft, malicious coding and outside or inside espionage as a way to express their creativity cum the anonymity nature of the cyber realm (Moore, 2012). Therefore, this theory is relevant in explaining the emergence of cybercrime because cyber fraudsters learn these deviant behaviours from their interactions with others and the environment around them. Cyber fraudsters acquire deviance behaviour on cyber or computer related crimes from people they associate within their daily lives. Today, people rely on computer devices to do almost every daily activity including communicating, studying, researching and working. Consequently, this environment provides a suitable environment for cyber fraudsters to thrive.

Methods

Research Design

The study adopted a descriptive survey research design employing the use of qualitative and quantitative methods of data collection for both primary and secondary data. This is to enhance the explanation on the prevalence and forms of cybercrime perpetrated by students in public tertiary institutions in Equity State, Nigeria. Both primary and secondary data was employed to gather information for the study.

Study Population

The study population comprises of the Nigeria law enforcement agencies (Nigeria Police and the Economic & Financial Crime Commission), suspected Cyber fraudsters and students in Public Tertiary Institutions in Equity State. The justification of using these categories of person(s) is because they are best suited to give relevant information to the study.

Population, Sample Size and Sampling Procedure

In selecting representatives from the public tertiary institutions, the study adopted a multi-stage sampling technique. Here, three hundred and ninety-two (392) copies of questionnaires was administered to students in the three purposive selected public tertiary institutions in the state and eleven (11) In-depth Interviews was conducted to compliment the questionnaire.

Methods of Data Collection

This part focus on the account of the instrument and methods that was adopted in the study to obtain the information required. The main purpose of the study is the prevalence and forms of cybercrime perpetrated by students in public tertiary institutions in Equity State. Therefore, both primary and secondary sources of data collection were adopted in the study. The primary source includes both quantitative and qualitative method in which questionnaire and In-depth Interview were used to gather data from respondents. Here, quantitative method was adopted in which three hundred and ninety-two (392) copies of questionnaires was administered to students in the three purposive selected public tertiary institutions in the state. While, qualitative method was an In-depth Interview which was conducted to compliment the questionnaire. The In-depth Interview was one-on-one discussion between the researcher and the respondent(s). The interview guide includes pertinent probing questions on the prevalence and forms of cybercrime perpetrated by among students in public tertiary institutions in Equity State. The secondary source was collecting relevant cybercrime record from the Nigeria Police, the Financial and Crime Commission (EFCC) and online articles or records for the research study.

Data Analysis

The data from questionnaire survey was analyzed with the use of statistical package for social science (SPSS version 20) software and presented as frequency percentage. Data collected through qualitative method (In-depth Interview) was transcribed from tape and it was compared with notes taken from the field. The transcribed interview was done manually using content analysis.

Results

Socio-Demographic Characteristics of Respondents in College of Education, Ekiti State University and Federal Polytechnic in Equity State

Table 1a: Percentage Distribution of Respondents on Socio-Demographic Characteristics.

Variables	**COEIKERE (N=71)**	**EKSU (N=196)**	**FEDPOLY (N=108)**	**Total (N=100)**
Age	No (%)	No (%)	No (%)	No (%)
Less than 20 years	21(29.6)	43 (21.9)	27 (25.0)	91 (24.3)
21-30	34 (47.9)	98 (50.0)	63 (58.3)	195 (52.0)
31-40	16 (22.5)	55 (28.1)	18 (16.7)	89 (23.7)
Gender				
Male	53 (74.6)	132 (67.4)	84 (77.8)	269 (71.7)
Female	18 (25.4)	64 (32.6)	24 (22.2)	106 (28.3)
Ethnic group				
Hausa	07 (9.8)	19 (9.7)	11 (10.2)	37 (9.9)
Igbo	11 (15.5)	26 (13.3)	22 (20.3)	59 (15.7)

Yoruba	33 (46.5)	113 (58.7)	46 (42.6)	192 (51.2)
Others	20 (28.2)	38 (19.3)	29 (26.9)	87 (23.2)
Religion				
Traditional	06 (8.4)	-	-	6 (1.6)
Orthodox Church	14 (19.7)	56 (28.6)	29 (26.8)	99 (26.4)
Pentecostal Church	21 (29.6)	70 (35.7)	41 (38.0)	132 (35.2)
Aladura Church	10 (14.1)	21 (10.7)	08 (7.4)	39 (10.4)
Islam	20 (28.2)	49 (25.0)	30 (27.8)	99 (26.4)

The Table shows the socio-demographic characteristics of respondents. Data on the age composition of respondents shows that more than half of the respondents from the three public tertiary institutions for the study fell within the age bracket of 21-30 years. This is to say that those between the ages of 21-30 constitute the highest percentage (52.0%) of the total respondents in the study. While a little below one-quarter were less than 20 years of age. Therefore, majority of the respondents are youths and as a result, within the active age group. This is as observed by Olive and Adware (2004) that cybercriminals in Nigeria falls within the youthful age. The youths at present have discovered different ways of using the internet in doing different types of criminal activities. This is because Nigeria youths are noted for being idealistic, adventurous, resourceful, inquisitive and proactive as envisaged by Adelman (1999) and youths are considered to be much inclined and, by efficacy of their education, constant and easy access to the internet, the clamour for material needs and the threat of impending unemployment, tempt the youths to engage in cybercrime as stressed Ngozi (2009). Nevertheless, Oyenuga, Odunaike and Oblation (2012) stresses that suspected cyber fraudsters starts at early age and declines with age; those who have stayed longer in the crimes drop out as they grow older and therefore, such was revealed in the study.

Data from the Table shows the gender disparity between respondents in the study. Out of 375 respondents, 71.7% were Male respondents while only 28.3% were Female. The striking disparity in gender composition of participants spread across the three selected public tertiary institutions in the state shows an overwhelming percentage distribution of Male respondents in the study. What this implies is that Male students show much interest in the study because they believe they have deep knowledge and practice of the subject matter more than the female students. Besides, Odom et al (2015) argued that cybercrime practice is dependent on gender. That is, male students engage more in cybercrime than female students.

Also, information on the ethnic group revealed that there was more Yoruba ethnic group in the study. Yoruba ethnic group has the highest percentage (51.2%) of the total respondents. Respondents with 15.2% constitute the Igbo ethnic group while the Hausa ethnic group represents the lowest percentage with 9.9%. Other ethnic groups in the study include Ebira, Calibre, Urhobo, I gala and I jaw with 23.2%. The dominance of Yoruba ethnic group is attributed to the fact that the study area is located in Equity State, Southwest, and Nigeria which is predominantly occupied by the Yoruba ethnic group.

The table shows the dominance of Christian religion from the three public tertiary institutions selected for the study. The table reveals an overwhelming percentage of Christian churches with 72.0% represented in the study. Among the Christian churches in the study, the highest percentage (35.2%) of respondents attends Pentecostal churches. The percentage for Islamic worshippers revealed 26.4% and the lowest percentage (1.6%) was Traditional worshiper.

Table 1b: Socio Background of In-depth Interviewees

S/N	Gender	Age	Occupation	Area	Education	Religion	Ethnicity
1	Male	23	Student	Ado-Ekiti	EKSU	Christian	Yoruba
2	Male	23	Student	Ado-Ekiti	FEDPOLY	Christian	Yoruba
3	Male	24	Student	Ado-Ekiti	FEDPOLY	Christian	Igbo
4	Male	24	Student	Ikere-Ekiti	COEIKERE	Christian	Yoruba
5	Male	24	Student	Ado-Ekiti	EKSU	Christian	Yoruba
6	Male	25	Student	Ikere-Ekiti	COEIKERE	Islam	Yoruba
7	Male	37	Police Officer	Ikole	B.Sc	Islam	Yoruba
8	Male	38	Police Officer	Okesa	B.Sc	Christian	Yoruba
9	Male	41	Police Officer	Ijero	HND	Christian	Yoruba
10	Male	45	Police Officer	Ikole	HND	Christian	Yoruba
11	Male	46	Police Officer	Ijero	B.Sc	Christian	Yoruba
12	Male	48	Police Officer	Okesa	B.Sc	Islam	Yoruba

The Table shows the social profile or characteristics of IDI participants for the study. It revealed that only Male students suspected to be involved in cybercrime participated in the in-depth interview and Male Police Officers also took part in the in-depth interview. Female students suspected to be involved in cybercrime were identified through snowball also, but were reluctant to participate for the interview. The justification for not participating as observed by the researcher was due to fear of the researcher being a spy for law enforcement agencies, not being bold enough or being shy to be interview, as a result, six (6) suspected cyber fraudsters were interviewed from the three public tertiary institutions in Equity State selected for this study. While for law enforcement agencies, only Male Police Officers also took part in the in-depth interview. This is because they were the Officers available and approved by their superior as at the time of the interview.

The age composition of IDI participants as stated in the table shows that the age range of students involved in cybercrime are between the ages of 23-25. What this implies is that those involve in cybercrime are within the youthful age as stated in table1a. While the age grade for law enforcement agencies shows the age range from 37-48. The implication of this is that, these officers are aware of cybercrime practice among students in the state.

The Table also explains the religion of participants. It shows that one student from College of Education, Ikere-Ekiti is a Muslim while other students are Christian. The table further shows the religion of Police Officer in which two of them are Muslim, each from Ikole and Okesa area command in Equity State and other Officers are Christian. Finally, the table explains the ethnicity of respondents as one person (a student from Federal Polytechnic) happened to be from the Igbo ethnic group while other participant (both students and Police Officers) are from the Yoruba ethnic group.

Prevalence of Cybercrime among Students in Public Tertiary Institutions in Ekiti State

Table 2: Percentage Distribution of Respondents on awareness of Cybercrime in the last five years

Respondents/Institutions	**Aware** **No (%)**	**Not Aware** **No (%)**
COEIKERE (N=71)	56 (78.9)	15 (21.1)
EKSU (N=196)	181 (92.3)	15 (7.7)
FEDPOLY (108)	91 (84.3)	17 (15.7)
TOTAL	328 (87.5)	47 (12.5)

In the Table, respondents across the selected tertiary institutions for the study assessed the awareness of cybercrime in the last five years and as a result, a larger proportion of respondents affirmed that they are aware of cybercrime in the last five years while, 12.5% claimed that they are not aware of the practice. Therefore, the implication of this finding revealed that cybercrimes has been in existence as a very larger percentage (87.5%) attests to its trend among students in tertiary institutions and the larger society. However, this was better captured in some of the in-depth interviews where participants expressed knowledge about cybercrime.

I think it started in late 21st century. I use to hear my mum saying it has been in vogue for years now and that people started it as online charity where fake pictures are sent abroad to NGOs

A male student from College of Education, Ikere-Ekiti

A participant further commented on this thus:

It started with some of our youth abroad who have the idea and they brought it to Nigeria. They believe that if it can be done in Nigeria, it will help unemployment instead of stealing. Today, many students in this citadel of learning (Equity State University) were able to sponsor their selves and feed their people. In fact, am happy that yahoo-yahoo is in existence.

A male student from Equity State University, Ado-Equity

Another contribution about the awareness of cybercrime perpetrated by students in public tertiary institutions showed that:

…initially, it started when the advent of technology like phone in which yahoo boys defrauds people using false identity to get phones and laptops from supermarket before it graduated into engaging with white men through internet.

A male student from Federal Polytechnic, Ado-Equity

Nevertheless, majority of the participants are aware of cybercrime in the last five years and as a result, the implication of this finding connote the perceptions of participants in the IDI about the time in which cybercrime has been in existed in Nigeria and also how cybercrime is been perpetrated through various means. Cybercrime is believed to assist unemployment in the country and as a result, eradicating poverty especially among youths in Nigeria. The in-depth interview explains the perception of suspected cyber fraudsters who sees their act as a means of earning a living. It also revealed the tools use in carrying out their illegal online activities within the cyberspace. Therefore, the existence of cybercrime among youths in Nigeria cannot be overlooked.

Table 3: Percentage Distribution of Respondents on the frequency of Media Report Cases of Student's Involvement in Cybercrime.

Frequency of Reported Cases	**Daily**	**Weekly**	**Monthly**	**Yearly**
	No (%)	**No (%)**	**No (%)**	**No (%)**
COEIKERE (N=71)	24 (33.8)	32 (45.1)	10 (14.1)	5 (7.0)
EKSU (N=196)	48 (24.5)	96 (49.0)	32 (16.3)	20 (10.2)
FEDPOLY (N=108)	29 (26.9)	50 (46.3)	19 (17.6)	10 (9.2)
TOTAL	101 (26.9)	178 (47.5)	61 (16.3)	35 (9.3)

The Table shows the percentage distribution of respondents on the frequency of reported cases on cybercrime among students in public tertiary institutions in the state. The study revealed that cybercrime among students in public tertiary institutions in Equity state is on weekly bases as majority with 47.5% confirmed it. Also, 26.9% claimed on daily bases, 16.3% settled on monthly bases and 9.3% believed it to be on yearly bases. This confirms the wide range of awareness about cybercrime in the state. More revealing is the impact of mass media that makes youths to be aware of or expose to cybercrime and the uncensored video and radio programs also encourage the perception of youths towards cybercrime. However, according to Okesola and Abimbola (2013), perpetrator(s) of cybercrimes are our brothers, friends, colleagues, distant relatives, tenants and neighbours. Therefore, cases of cybercrime are not farfetched and this was further stressed the in-depth interview;

...of course it is prevalent in Equity state, about 85% of students engage in it. If you move around, you will see these yahoo boys flaunting their wealth. You see a young boy too who has no job or a secondary school students who should be studying chasing girls or going to club.
A male student from College of Education, Ikere-Ekiti
Another participant submitted that:
It is like a trend now. It is perpetrated by the youths especially those between 18 years and above. It is the students and youths. Some married men engaged in it but not as common as the youths. It is very common especially the youth and i will give its prevalent 80% in Ekiti State.
A male student from Equity State University, Ado-Equity

Table 4: Percentage Distribution of Respondents on the Prevalence of Cybercrime among Students in Tertiary Institutions.

Prevalence of Cybercrime	**Prevalent** **No (%)**	**Not Prevalent** **No (%)**
COEIKERE (N=71)	56 (78.9)	15 (21.1)
EKSU (N=196)	174 (88.8)	22 (11.2)
FEDPOLY (N=108)	93 (86.1)	15 (13.9)
TOTAL	323 (86.1)	52 (13.9)

Data from the Table revealed an overwhelming percentage distribution of its prevalence among students in public tertiary institution in Equity state. What this implies is that, majority from sampled survey believed that cybercrimes is rampant among students in public tertiary institutions in Equity State and this is said to be true because as at the end of the first quarter in 2016, Nigeria was ranked 3rd in the world and Nigeria youths, has been the major factor facilitating the utilization of the internet in defrauding unsuspecting person(s) around the globe

(Nigeria Communication Commission, 2017). Participants from the in-depth interview further stressed the prevalence of cybercrime among students in public tertiary institutions in the state.

It is very common among we youths especially we students in tertiary institutions and i will rate its prevalent 80% in the State.
A male student from College of Education, Ikere-Ekiti
Participant from Federal Polytechnic contributed that:
I will say it's more than prevalent because about 90% students/youths are yahoo guys, though; females are also involved but not rampant as guys.
A male student from Federal Polytechnic, Ado-Equity
Another participant stressed thus:
It is very rampant. On a scale of hundred among male student in Equity State University, I can say 85% of the boys are engage in cybercrime while females too are involve but not up to the male students.
A male student from Equity State University, Ado-Equity
Forms of Cybercrime among Tertiary Institutions Students in Equity State

Table 5: Percentage Distribution of Respondents on the Types of Cybercrimes Perpetrated by Students in Tertiary Institutions in the State

Types of cybercrime carried out	**Advance Fee Fraud**	**Hacking**	**Piracy**	**Online Charity**	**ATM/BVN Fraud**
	No (%)	**No (%)**	**No (%)**	**No (%)**	**No (%)**
COEIKERE (N=71)	37 (52.1)	7 (9.9)	-	10 (14.1)	17 (23.9)
EKSU (N=196)	84 (42.9)	31 (15.8)	-	43 (21.9)	38 (19.4)
FEDPOLY (N=108)	38 (35.2)	21 (19.4)	10 (9.3)	12 (11.1)	27 (25.0)
TOTAL	159 (42.4)	59 (15.7)	10 (2.7)	65 (17.3)	82 (21.9)

The Table shows the types of cybercrime perpetrated by students from the selected public tertiary institutions in the state. The study revealed that 42.4% of the total respondents believed that the Advance free fraud is the common type of cybercrime perpetrated by students in public tertiary institutions in the state. The table also revealed a low percentage distribution of piracy. As a result, the implication of the information is that duping unsuspected victims is more prevalent and easy to carry out than others. This is because these cyber fraudsters extort money from their victims promising to be in love with them. Nevertheless, a male student from Equity State University has this to say during an in-depth interview on the type of cybercrime perpetrated by students;

Internet dating also known as advance fee fraud is the most common among students, in which they fake someone's identity (ID) to extort money from someone online but not under the act of force. The victim only give out the money thinking the person is in love with him/her. It is not a force. This thing has different format and it can be spread to 50 people in which one can have 3 to 4 girls using the same format.

A male student from Equity State University, Ado-Equity

A participant from the Nigeria Police submitted that:

It is the Advance fee fraud which is the internet dating or the ATM/BVN, but hacking is another system which is not so pronounce in Nigeria unlike the developed world or countries because they don't have the technicality. It involve building a software program before one can hack a system and hacking bring in money and it's not as rigorous as the advance fee fraud. Besides, we have recorded one case like that where a boy hacked into First bank Nigeria PLC because he is very brilliant in building software

A Male Police Officer

Table 6: Percentage Distribution of Respondents on the Life Style of Students Practicing Cybercrime

Lifestyle of Suspected Cyber fraudsters	**Always on Net** **No (%)**	**Spending Lavishly** **No (%)**	**Riding Latest Car** **No (%)**	**Mainly Clubbers** **No (%)**	**Indulging in Ritual** **No (%)**	**Tyrant in Class** **No (%)**
COEIKERE (N=71)	18 (25.3)	32 (45.1)	9 (12.7)	10 (14.1)	2 (2.8)	-
EKSU (N=196)	42 (21.4)	76 (38.8)	31 (15.8)	20 (10.2)	10 (5.1)	17 (8.7)
FEDPOLY (108)	28 (25.9)	53 (49.1)	10 (9.3)	17 (15.7)	-	-
TOTAL	88 (23.5)	161 (43.0)	50 (13.3)	47 (12.5)	12 (3.2)	17 (4.5)

The findings from the Table above indicated that spending lavishly is the life style of students indulging in cybercrime. The table demonstrated that majority (43.0%) from the selected sampled survey affirm that spending lavishly is the life style of suspected cyber fraudsters. What this implies as shown in the table is that people are valued in terms of what they posses and command economically. Zero Tolerance (2006) opined that youths indulge in cybercrime in order to survive or live a life of splendour. However, money is believed to be the major motivator for many cybercriminals as posited by Edward (2016). In the submission from one of the in-depth interview, it was noted that:

Maybe because of poverty and some people love the use of expensive things and as a result, engage in it. Personally, I don't place judgment on people especially when I don't know their source of income. In Equity State, most guys that fluent their wealth are yahoo boys but there are *legitimate ones. It's just like the saying, "things you don't work hard for are spend lavishly". People or yahoo guys see flaunting of wealth as a competition. Imagine a guy saw his peers with a jeep and he has no car but have the resources like computer, he will definitely one to. It challenges others to engage in it. They (yahoo boys) use it to oppress people by lavishing their wealth. This is the reason why many youths engage in it because they saw how these guys display their wealth.*

A male student from College of Education, Ikere-Ekiti

Another participant submitted that:

....it has bad influence on the youth because seeing your peers spending lavishly, you will want to do like them. Some people actually go into it for different reasons. In the part of the youths, some wants to measure up with their peers and also want to live an extravagant life. They want to acquire expensive things. Some wants to feel among.

A male student from Equity State University, Ado-Ekiti

Discussion

The findings from this study also revealed that cybercrime is trending among students in public tertiary institutions in Equity State and by extension, in Nigeria as an overwhelming percentage of respondents affirmed that they have heard of cybercrime in the last five years. This is true as envisaged by Asocial (2010) that students are aware of cybercrime due to mass media programs. Furthermore in the study revealed that cases of cybercrime are on weekly bases. In the study, 47.5% respondents believed that reports cases are on weekly bases. Nevertheless, this study earlier pinpointed Okesola and Abimbola (2013) view, that the perpetrator(s) of cybercrime are not far-fetched as they are our brothers, friends, colleagues, distant relatives, tenants and neighbours. Also, the study revealed the prevalence of cybercrime among students in public tertiary institutions in Equity State. It shows that a very larger proportion of respondents confirmed that the practice is rampant in the state. Recently, the Nigeria Communication Commission (2017) says that Nigeria is currently rank 3rd globally in cybercrimes behind United Kingdom and United State of America in which Nigeria has lost #125 billion to cybercrime as estimated in 2015. Its prevalence is due to the fact that many youths or students see cybercrime as an occupation. Also, the study revealed that 42.4% of the total respondents believed that the Advance free fraud is the common type of cybercrime perpetrated by students in public tertiary institutions in the state. The table also revealed a low percentage distribution of piracy. As a result, the implication of the information is that duping unsuspected victims is more prevalent and easy to carry out than others. This is because these cyber fraudsters extort money from their victims promising to be in love with them.

Conclusion

So far, the researcher conclude that cybercrime is a trend and still very rampant among youths or students in Nigeria considering the facts and figures recorded and has contributed negatively to the society. Though, it cannot be eradicated but can be adequately control if law enforcement agencies were trained on the use of technology as the constraints confronting them in doing the needful is should be critically addressed by the policy makers. Nigeria law enforcement agencies are endowed with certain responsibility in controlling the spread of cybercrime among youths or students in Nigeria, as this will sensitized them to collaborate with other sister agents in controlling cybercrime effectively.

Recommendations

To reduce the prevalence of cybercrime among youths or students in Nigeria, there should be adequate technological training of law enforcement agents in forensic department. Nevertheless, in the process of recruiting law enforcement agents, those with computer know-how should be enlisted adequately.

It is important and timely to adopt and create new law enforcement agencies that will be saddled to regulate and control certain cyber activities as apprehending cybercriminals becomes difficult due to the complexity in cyber space.

There should be a more proactive approach that will allow law enforcement agencies to track and investigate students involve in cybercrime within and outside the institution. Besides, most of these students that practice such act can be easily tracked within their hostels in the institutions.

School management should be allow to report students detected to be involve in cybercrime as to averts its escalation, because by doing so will reduce the perpetration of cybercrime within the school. This can only be achieved through effective collaboration between school management and law enforcement agencies.

References

Adelman, I. A (1999).*Youth and City: An Urban Environment Perspective, Workshop Proceedings on Youth and City: A Study of Lagos*. Development Researchers' Cooperative, Lagos.

Asocial, M. O (2010). Enhancing National Development and Growth through Combating Cybercrime/Internet Fraud: A Comparative Approach. *Journal of Social Science, 23(1):13-19.*

Basil U. (2016). Cybercrime Act does not create an Enforcement Agency. Retrieved on the 2nd of August, 2016 from *www.thisdaynewspaper.com*

Consumer Reports State of the Net (2007). *U.S. Nationally Representative Survey of more than 2000 America Households*. Consumer Reports National Research Centre

Felon, M and Cohen, L. (1979).*Social Change and Crime Rate Trends: A Routine Activity Approach*. American Sociological Review

Bengal, S., Babatunde, S, and Bankable, F (2012). *Economic Cost of Cybercrime in Nigeria*. University of Toronto. Monk School of Global Affairs

Martin, L (2016). General Introduction to Cybercrime Effects in Nigeria Sector. Retrieved from *www.MartinLibrary.com*

McLeod, S. (2016). Bandera-Social Learning Theory. Retrieved from *www.simplypsychology.org/bandura*.

Moore, R. (2012). *Cybercrime: Investigating High-Technology Computer Crime*. Burlington, MA: Elsevier Science.

Ndubueze, P. N (2013). Social Values and the Yahoo boys' Subculture in Nigeria: Towards a Paradigm Shift for National Value Re-Orientation. *The Nigerian Journal of Sociology and Anthropology. Vol. 11, No 1*

Gnosis, G. E (2009). Globalization and Transnational Advance Fee Fraud: A Study of Perceptions of Undergraduates in South-eastern Nigeria. *The Nigerian Journal of Sociology and Anthropology. Vol. 7, No 1*

Nigeria Communication Commission (2016). A Summary of the Legislation of Cybercrime in Nigeria. *Retrieved on the 26th of July, 2016 from www.thecommunicatormagazine.com*

Odom, A. I. and Odom, C. R. (2015). The Extent of Involvement in Cybercrime Activities among Students' Tertiary Institution in Enugu State of Nigeria. *Global Journal of Computer Science and Technology: H Information & Technology. Vol. 15 (3): 1-6*

Domes, J. O (2014). A Socio-technological Analysis of Cybercrime and Cyber security in Nigeria. *International Journal of Sociology and Anthropology. Vol. 6(3), pp.116-12*

Okesola, F. B and Abimbola, K. A (2013). The Nature, Causes and Consequences of Cybercrime in Tertiary Institutions in Zaria-Kaduna State of Nigeria. *American International Journal of Contemporary Research 3(9), 98-114*

Olive and Areole (2004), Cybercrime Embarrassing for Victims. Retrieved September 2011 from *www.Heraldsun.com*

Ovum, B. and Ajani, J. A. (2013). Traditional Values, Beliefs and Reliance on Indigenous Resources for Crime Control in Modern Southwest Nigeria. *Africa Research Review: An International Multidisciplinary Journal, Ethiopia Vol. 7(1) 73-94.*

Ova, J. (2001). '*Internet Banking: Practices and Potentials in Nigeria'*. A Seminar paper presented at the Institute of Chartered Accountants of Nigeria (ICAN), Lagos

Yesinia, F (2015). *Nigerian Internet 419 on the Loose*. USA: Gettysburg PA

Sutherland, E. H (1960). *"A Theory of Differential Association."Criminological Theory: Past to Present*. Ed. Cullen, F.T and Agnew, R. Los Angeles: Roxbury Company, 2006. 122-125

The news (2016). Cybercrime: Nigeria's Ranking gets Worse. *Retrieved from www.thenewsnigeria.com.ng on the 28th of June 2016*

Umeozulu, F. (2012). *Perceptions of Cybercrime among Nigeria Youth*. Maori-Nike, Caritas University.

Zero Tolerance (2006). *Retiree in Trouble over Internet Fraud*. Economic and Financial Crime Commission, Vol. 1, No 2: 219-225