CYBERCRIME: A THREAT TO A MORAL SOCIETY

[1]D.D. Wisdom, [2]E. A Ajayi, [3]M. K. Hamza, and [4]O. O. Odewale
[1]Department of Mathematics, Computer Unit, Usmanu Danfodiyo Email: danieldaudawisdom1@gmail.com
[2]Faculty of Computing and Informatics, Multimedia University, Cyberjaya Campus, Persiaran Multimedia 63100 Malaysia:ebeconsult@myself.com
[3]Software Dev/Main unit, MIS, Usmanu Danfodiyo Email: kabiru.mohmmed@udusok.edu.ng
[4]Computer Science Department, Ibadan City Polytechnic, Alakia/Iyana church Road, Ibadan, Oyo State.
Email: omolaraodewale@gmail.com

ABSTRACT

Several internet related crimes known as cybercrimes are committed daily in various ways such as Spamming, IP Spoofing, fake bank alert messages (SMS) /unsolicited SMS requesting you to provide bank details as Bank Verification Number (BVN), Advance fee fraud, identity theft, piracy, pornography, hacking, fraudulent e-mail related SMS, forgery such as fake documents as Certificate etc. Cybercrimes is on the increase, and is gradually becoming a threat to our moral life and the society at large. The increase number of cybercrime rate is an open field of ongoing research studies. This paper have propose a new approach that emphases on the prominent cybercrimes carried out in some major areas in Nigeria, precisely within secondary school students and presents a study of cybercrimes in these institutions within kebbi State and sokoto state. Presents a new approach to Cybercrime prevention in order to efficiently combat cyber related crimes in Nigeria.

Keywords: Cybercrime, Advance fee fraud, Identity theft, IP Spoofing, Pornography.

1.0 Introduction and Background

A moral society is a pedestal for technology and social development. While the trend of technology increases threats as cybercrime are major setbacks.

Since Cybercrime or Cyber related Crimes are equally on the raise with much severe effect on the community at various levels at large. Students at almost all academic levels are in one way or the other involved in Cybercrime.

And these prevailing epidemics have left no level or race unaffected. As at 2003, the United States and South-Korea have the highest cyber-attacks of 35.4% and 12.8% respectively, according to [1]. With the population of Nigeria placed at 180 million from the last census carried out in 2015/2006, a recent statistics revealed that about 28.9% have access to the internet [2]. It was also proven that 39.6% African users of internet are actually Nigerians, hence, the high increase in the rate of internet crime in Nigeria [2]. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the younger generation of students; more especially the secondary school students.

Cybercrime defined as type of crime committed by criminals who take advantage of a computer devices as tools 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 etc. [3]. Cyber-crime evolves from the wrong application or abuse of internet services. The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s [3]. Since these computers were not connected to the internet or with other computers, the crime was committed by the employers within the company; hence it was referred to as computer crime rather than cybercrime.

The rest of the paper is organized as follows: section 2. Detection of cybercrime, Section 3. Presents literature review, section 4. Methodology, Section 5. Results and Discussion, Section 6. Concludes our Research work.

1.1 Basic Concept of Cybercrime

Cybercrime is an emerging trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crimes usually require a hectic task to trace. Cybercrime may be divided into two categories:

1. Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, malware etc.
2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Advance fee fraud such as Yahoo Yahoo, Money theft through the ATM, Fake documents or Certificates, SMS requesting you to provide bank details as Bank Verification Number (BVN).

1.2 Causes of Cybercrimes in Nigeria

The following are some of the few newly identified causes of cybercrimes [2],[17].

1. Unemployment is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 40 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities as a means for their daily survival.

2. Quest for Wealth is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to meet up with their rich counterparts by engaging in criminal activities such as cybercrimes.

3. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go unpunished. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unrewarded for their committed crimes.

4. Incompetent or unskillful security on personal computers. Some personal computers do not have proper or competent security controls, it is prone to criminal activities hence the information on it can be stolen or exchanged unnoticed.

5. Marriage: most of the youth get married with the intension that with time they will eventually secure a gainful employment after a period of time all of which never happened. Thus, this becomes difficult for them to take care of their families leaving them with the temptation or no option than
to end up in cyber related crime as a source of their livelihood.

6. Age: It's observed from our research that age significantly has an influence on an average youth in their involvement in cybercrimes.

1.3 Numerous Cybercrimes in Nigeria

For Several decades, the internets have experienced an increase growth with the number of hosts connected to the internet increasing daily at a speedy rate. As the internet grows to become more accessible and more facilities become reliant on it for their daily operation, likewise the threat such as cybercrime. In Nigeria, cybercrime has become one of the main

avenues for stealing of money and business spying. According to Check Point, a global network cyber security vendor, as of 2016, Nigeria is ranked 16th highest country in cyber-attacks vulnerabilities in Africa [4]. Nigerians are known both home and abroad to be rampant perpetuators of cybercrimes. The number of Nigerians caught for duplicitous activities carried by broadcasting stations is much more in comparison to other citizens of different countries. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, these sectors such as the banking, e-commerce and education sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its previous ones. Hence, in this section, prominent specific ways in which cybercrimes are mostly carried out in Nigeria are presented.

1.3.1 Banking Sector

The life wire of the banking sector is the internet. Presently, banks all over the world are taking advantage and incorporating opportunities brought about by Electronic banking (e-banking) which is believed to have started in the early 1980's [5]. As the security level in this sector becomes stronger, the strength and tactics of these fraudsters increases also. Various threat attacks have been explored in which, many of them are successful. Generally, cybercriminals carry out fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or/and transfer funds to another bank account without rightful authorization. However, in some rare cases in Nigeria, the intention of cyber-criminals is to cause damage to the reputation of the bank by denying service to users [6] and sabotaging data in computer networks of organizations.

1.3.2 Bank Verification Number (BVN) Scams: The BVN is a biometric identification system which consists of an 11-digit number that acts as a universal ID across all the banks in Nigeria. BVN was implemented in 2015 by the Central Bank of Nigeria. It was introduced to link various accounts to the owner thereby ensuring that fraudulent activities are minimized. For fraudsters, opportunities to extort money and to carry out other fraudulent activities arose from the implementation of the BVN. It was detected that fake and unauthorized text messages and phone calls were sent to various users demanding for personal information such as their account details. In addition, phishing sites were created to acquire such information for unhealthy activities on the bank account of individuals.

1.3.3 Phishing

Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorized businesses and financial institutions that are victimized [14]. Phishing scams are universal and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. In this jet age of technology, hoi polloi subscribe to a plethora of sites using their email addresses and are therefore expecting to receive mails of updates of their membership or subscription. So it seems natural when users get regular mails from such organizations. Likewise fraudsters have also devised a means to mimic authorized organizations and retrieve confidential information from clients. In Phishing mail messages, the fraudsters' tries to find a way to convince and gain the trust of users. In Nigeria, phishing mails are mostly carried out on bank customers either through mail, text Messages or phone call requesting individual bank information for the purpose criminal activity. In some cases social media platforms like WhatsApp, Facebook, etc are used to initiate communication just to establish trust and confidence, there by exploiting individuals for the said motive.

1.3.4 Cyber-theft / Banking Fraud

Hackers target the vulnerability-ties in the security of various bank systems and transfer money from uncountable accounts to theirs. Most cyber-criminals transfer little amounts like 5 naira which are sometimes overlooked by the user without questions raised by the

users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most fraudsters.

1.3.5 Sales Fraud & Forgery

In our society today, fraudulent sales of products that do not exist or that are imitations are increasingly common. The purchase of an item before actually seeing it has created ways for fraudsters to make money via the sale of unoriginal products or in some cases, the total absence of the product. Many persons have fallen victim of this particular crime on popular e-commerce websites, where the hackers' makes used of a cloned websites to perpetrates there crimes.

1.3.6 Data and Airtime Time (DAT) theft from service providers

This is a widespread scam among the youths of now are days. They illegally gain access to "Cheat codes" and unlawfully use them to gain thousands of mobile data and unlimited airtime without making the necessary payment. Also, cyber cafes have developed means of connecting to the network of internet service providers unlawfully.

1.3.7 Education Sector and Cybercrime

The educational sector in Nigeria suffers greatly from electronic crimes which are perpetuated mostly by students in tertiary institutions.

1.3.8 Cyber-Plagiarism

Information housed on the internet has made an effective alteration on the methods in which people educate themselves. The term 'Copy and Paste' is the most common phrase used when referring to cyber-plagiarism. Cyber-plagiarism can be defined as copying and pasting online sources into word processing documents without reference to the original writer /owner. In the educational sector in Nigeria, students, particularly those in the tertiary institutions carry out this crime without enforcing the due penalty.

1.3.9 Pornography

Cyber-pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials de-picting children engaged in sexual acts with adults or adults as well. Cyber-pornography is a criminal offense, classified as causing harm to persons, especially the youth.

1.3.9.1 Bank Cards Theft

The theft of bank cards has evolved from the physical theft of the card to simply the theft of the numbers. Today, bank card hackers do not need to be in the same country to steal other people's identities. Fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS, or at the ATM. According to the Federal Bureau of Investigation (FBI), a method known as ATM skimming can be used and it involves placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine (FBI, 2011).

Also, another cybercrime carried out via this means in Nigeria includes internet order fraud. Internet order frauds involves fraudster inputting stolen cards numbers on online comer

1.3.9.2 Cybercrimes on Social Media

In Nigeria, Social networks have gained a very high ground in every sector. The banking industry, government, business, universities use this platform to promote and communicate with each other. Social networking sites such as Facebook, Twitter, LinkedIn and Instagram serve as a fertile ground for cybercriminals to launch new attacks. Users create semi-public profiles and can directly communicate with friends without restriction [7].

1.3.9.3 Nigerian-Prince (Beneficiary of a will) Scam:

The fraudsters send messages through social media sites speculating that the receiver is a named beneficiary of a huge some of amount or an estate from a will left behind from a deceased descendant.

1.3.9.4 Charity Funds
Fraudulent people host fake social network pages for charity soliciting for money. In most cases, these fake social pages are backed up with pictures showcasing various illnesses. Many kind hearted people donate to this cause thereby increasing the pockets of cyber criminals.

1.3.9.5 Cyber-Stalking, harassment and Blackmailing Scam
This are threatening and blackmailing acts carried out on the internet by fraudsters on a victim. In most cases, the perpetuator's identity is unknown by the use of a false alias or by blocking the identity by keeping all information hidden.

1.3.9.6 Social-Hi-Jacking
This is a major crime all over the world. Many social networking pages have been hijacked by hackers who demands money in turn for releasing the personal social page. This has occurred in sites like Twitter, Facebook and Instagram. These fraudsters go as far as sending messages from the authorized page to friends and family requesting for money or any other kind of assistance. Also, another common scenario also occurs when the fraudster creates a social page pretending to be someone else especially celebrities.

2.0 Detection of Cybercrime
The following are some of the ways by which cybercrimes can be detected [8].

2.1 Email inspection: inspecting your mails before opening is a very useful way of detecting unusual or strange activities. Email spamming and cyber stalking can be detected by carefully investigating the email header which contains the real email address, the internet protocol address of the sender as well as the date and time it was sent.

2.2 Intrusion Detection System (IDS)
This is applicable for more serious attacks like breaking into a bank network to steal customer's sensitive data which cannot be discovered by mere inspection or reviewing. Intrusion detection techniques such as Honey pots, Tripwires, Anomaly detection systems, Operating system commands and Configuration checking tools are always employed.
Another well-known system is Snort; it is a robust open source tool which exists for monitoring different network attacks [9]. It was first developed in 1998 and gradually evolved into a mature software and even better than many commercial IDS. The system employs the rules established by the administrator to monitor traffic and detect strange behaviors.

2.3 Detection of Cybercrime
Cybercrime cannot be easily and completely wiped out, but can be reduced. However, collaborative efforts of individuals alongside with government intervention could go a long way to reduce or minimize it to a reasonable level. Measures to take can be categorized into two [3]:
1. Governments intervention: Although the country has found herself in great mess by the inability of the government to provide basic necessary amenities such as jobs, security and the likes for her citizens which indirectly has led to high rate in cybercrime, there is still need for the nation to come up with adequate laws to tackle this issue. These laws should be formulated by the government and should strictly be adhered to. However, it is worthy to note that a bill was passed in the year 2015 that would protect and punish electronic fraud and other cyber related crimes. The full implementation of this bill will hopefully bring a strategic approach to fight against cybercrime. Some of the bills are highlighted below: There will be seven years jail term for offenders of different types of computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting.
Defines the liability of service providers and ensures that the use of electronic communications does not compromise national interest. It provides a legal framework to punish cyber criminals thereby improving electronic communication.

It specifies all criminal acts and provides guidelines for the investigation of such offences. If these laws are effectively enforced, cybercriminals will be deterred and penalized. This will indirectly reduce the incident of cybercrimes, increase customer's confidence while transacting business online and also correct the negative impression about Nigeria and the citizens.

2. Individuals on their part should ensure proper security controls and make sure they install the latest security up-dates on their computer systems. In addition, they should observe the following [1]:
(i.) Carefully select the sites you visit. (**ii.)** Do not visit an untrusted site. (**iii.)** Avoid visiting a site by clicking on a link you find in your email, found on a Facebook page, or on an Advertisement.
(iv.) Avoid pirated software and never disclose your Personal Identification Number (PIN), bank account and email access code to unknown persons.
(v.) Always ignore any e-mail requiring your financial information. Do not send sensitive information in an email since its security cannot be guaranteed.
(vi.) Use strong passwords that are difficult to guess and employ a combination of characters (upper case and lower-case letters), numbers and symbols.
(vii.) Avoid inputting your information in a pop-up. If you have interest in any offer you see on a pop up, it is always safer to go directly to the website of the retailer.

2.4 Examination of Cybercrimes in Secondary Schools within Kebbi and Sokoto State

The aim of this research study is to evaluate the level of involvement of students in cybercrime and to determine their vulnerability in such crimes. This study adopts various research questions carried out among students in Kebbi and Sokoto-state. The approach employed in the distribution and answering our fact finding Questionnaire, was interview base for those secondary school students who unfortunaly cannot fill a Questionnaire by themselves, we ask these individual students Questions as guided by the Questionnaire and fill the appropriate Colum. While some of them who can fill the questionnaire were given to fill by themselves. We also decided to administer this questionnaire to students in their individual homes, as we discovered at the cause of this research study that secondary school students tries to shield their real salve in school. Each institution is well populated; however, and are more real at home since they are at liberty at home. Our research study covers a total of 52 students Questionnaire which were served. The questionnaire consisted of 15 questions that cut across all aspects of cybercrime in Nigeria especially within secondary school institutions. Each question has an option while others are multiple choice Questions.
language for implementation of the system is PHP and java. MySQL was used as the database. Hardware used for implementation has inbuilt webcam or attached digital camera for facial image capturing, a GPS sensor to locate a cyber-user point as well as a fingerprint scanner. The study was modeled to provide interfaces and capture the digital signatures for every information sent to the cyberspace, the user fingerprints and facial image are designed as the mandatory login parameters. Thus, the models identifies and record the geographical location of each user, the MAC address of the system used, the date,

3.0 Related Literatures

This section presents a review of related literatures on cybercrime within and outside Nigeria. The review highlights the achievements and open issues of each scheme as directions foe future research.
In [10], Cyber Crime Detection and Control Using the Cyber User Identification Model was propose to identify cyber users as a strategy to detect and control cybercrime. Object oriented paradigm of system analysis and design methodology was adopted. The crime scenes considered for detection are phising, identity theft and data theft. The

time and the kind of action performed by the user while online, and then
record any possible security threats for more findings by the cybercrime investigators.
In [11], social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals was proposed to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrimes. The study claw upon a basic principle of categorization with motivational theories, to offer a tripartite conceptual framework for grouping cybercrime nexus. The research contends that cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical.

In [12], Preparing South Africa for Cyber Crime and Cyber Defense propose that many developing countries are either not properly informed or adequately aware by both knowledge and legislation, in the circumstance of cyber-attack on a national level. And even if these countries realize the threats, the time to react is such a long time due to consultation and legislative processes, that the legal systems provide little support to ensure timely and necessary counter-measures. This research address this
Problem by looking at the impact of technological revolution on cybercrime and cyber defense in a developing country and will measure the relevant South African legislation, and also look at the influence of cyber defense on the international position of the South African Government.
In [14], Causes of Socioeconomic Cybercrime in Nigeria was propose to explore parents' perceptions of the factors that cause socioeconomic cybercrime in Nigeria. The study investigates, individuals' moral-standard-levels, which shape their volatile capacities, revealed to be mostly developed in childhood. The empirical basis for this research was a face-to-face interview with 17 Nigerian parents regarding children's vulnerability to involvement in cybercrime. Drafting upon qualitative data, the study argues that a complex web of familial factors and structural forces, alongside cultural forces, explains the degree of cybercrime involvement on the part of the Nigerian youths.
In [15], Analyzing Cyber Crimes Strategies: The Case of Phishing Attack was propose to analyze various phishing attack styles which includes Nigeria, Ghana, Chinese and Russian cybercrime styles. Due to the abundance of learning resources Russians and Chinese were found to be using more advanced techniques than that of the Ghanaians and Nigerians who has limited resources.

In [18], U.S. And EU Legislation on Cybercrime was propose that the U.S. legal systems and law enforcement agencies appear to be left behind in their efforts to capture and prosecute cybercriminals. This research study both U.S. and EU cyber legislations and how effective they are in controlling cybercrimes. The factors affecting U.S. From taking a leadership role in fighting cybercrime is reviewed. EU legislations were compared to see if U.S. can benefit from EU Pattern conceptualization.
In [20], Electronic Banking and Cyber Crime in Nigeria a Theoretical Policy Perspective on Causation was propose to assess cybercrime and its impact on the banking institutions in Nigeria. The research investigates the existing policy framework as well as assessed the success of the institutional countermeasures in combating cybercrime in the banking industry. The study examines cybercrime policy issues and provides insight into how cybercrime impacts on E-banking from a Nigerian perspective. Social theories were used to explain causation with a view of guiding policy makers on behavioral issues that should be considered when formulating policies to address cybercrime activities in Nigeria.

4.0 Methodology

The method employ for this research study was Questionnaire base. We developed a research Questionnaire that comprises of 15 fact finding questions and administered them to secondary

school students within Kebbi and Sokoto State. The method of administering our questionnaire was Question base to some of the students who could not fill the questionnaire by themselves while others fill by themselves. The choice of administering our Questionnaire to students at home was for the students to be at liberty to answer our questionnaire sincencerly. As research have revealed that most of the secondary school students tries to pretend who they are not in actual sense in their various schools. While the presence of the teachers could be a factor that may not allow students to confidently fill the Questionnaire due to the nature of some questions asked from the questionnaire that requires confidentiality.

5.0 Result and Discussions

In this section we present detail discussion of our results as well as definition of terms and meaning. Table 1-6 contains definition of terms, description and meaning respectively.

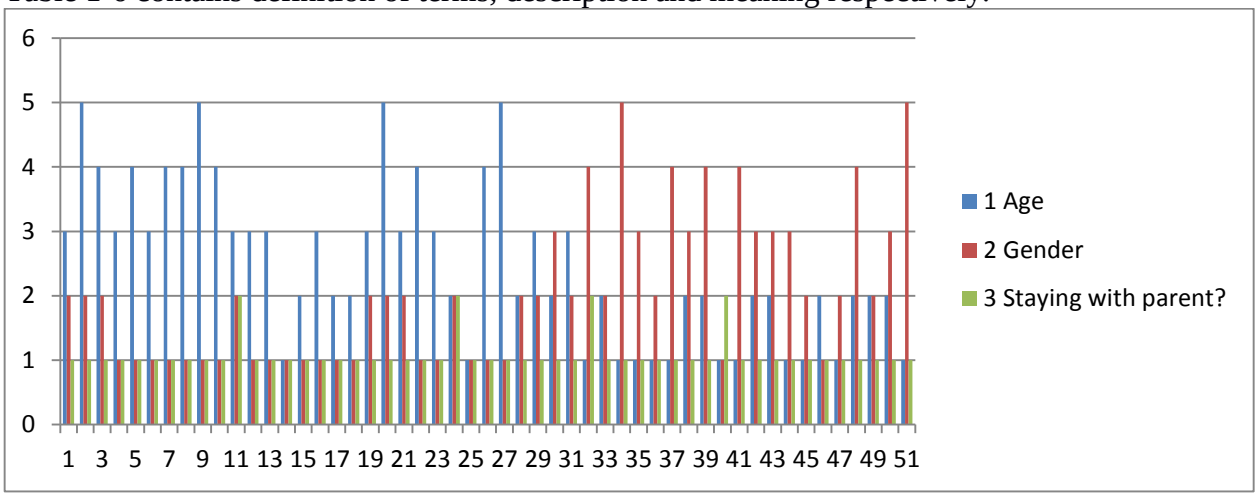


Figure 1. Above shows the relationship between Age, Gender and students who stay with their parents and likewise those that stays away from their parents. The age depicts the different individual age range and its effect on the students who stay with their parents and those that do not. The research study revealed that students within the age of 15-81 (3), start having interest in staying alone, some of which easily subject them to become expose to cyber related crimes at early age. The study also showed that male students are more easily prone to cyber related crimes than the female.

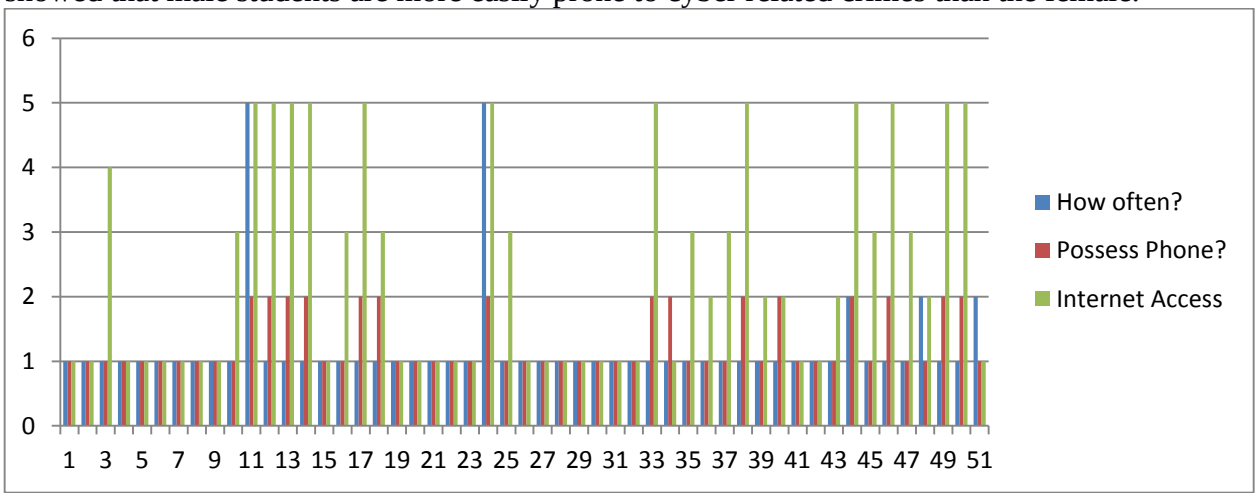


Figure 2. Above depicts the relationship between how often students stays with their parents, how many of them possess mobile phone, and how often students access the internet with their mobile phone. The study above proves that student within the age of 15-18(3) and above access the internet all the time, while student within the age of 10-12(1) and students within the age of 12-14(2) access the internet seldom. Since most of them within this age group collects phones from their parents in

an opportune time to use, but majority of them at this age do not have their own personal mobile phone.

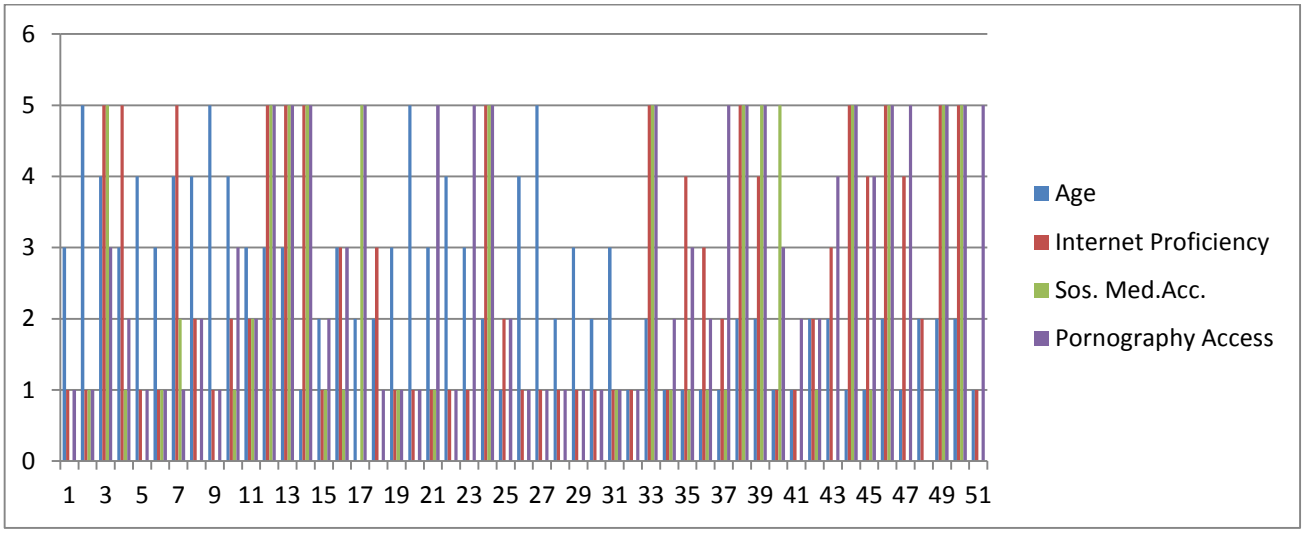


Figure 3. Above depicts the relationship between age, how many social media accounts a students has, and how often they visits sites related to pornography and their understanding of the internet as well. The study revealed that Students within the age of 15-18(3) and above have more social media accounts and are exposed to pornography access mostly, while students within the age of 10-12(1) and students within the age of 12-14(2) are less expose. But as they advance in age, it is observed that the rate of exposure to pornography increases and the number of their social media accounts as well, as seen above in figure 3.

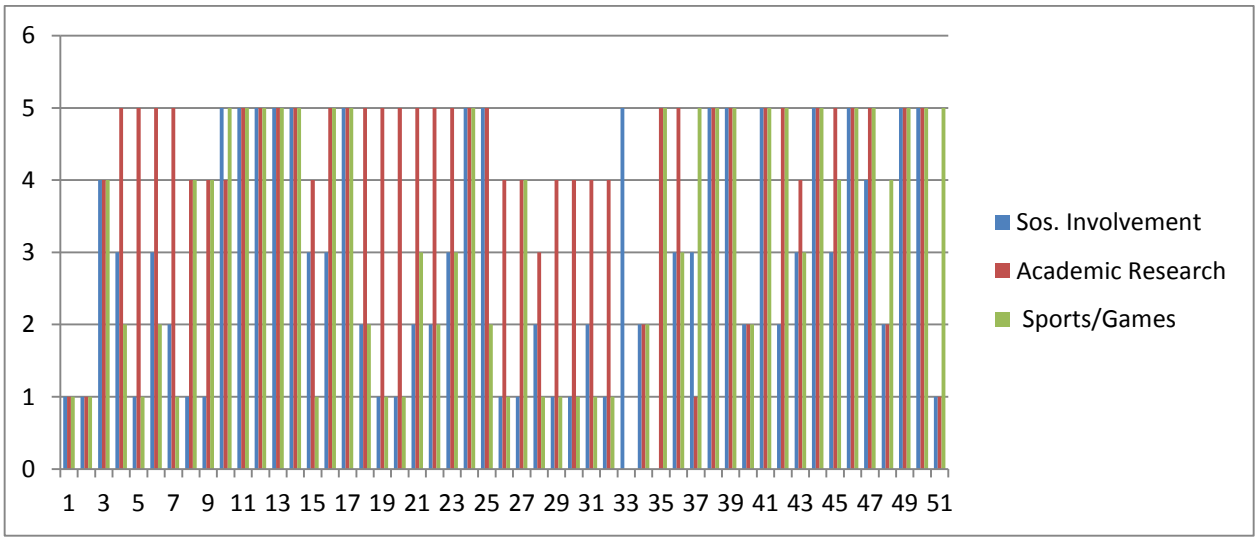
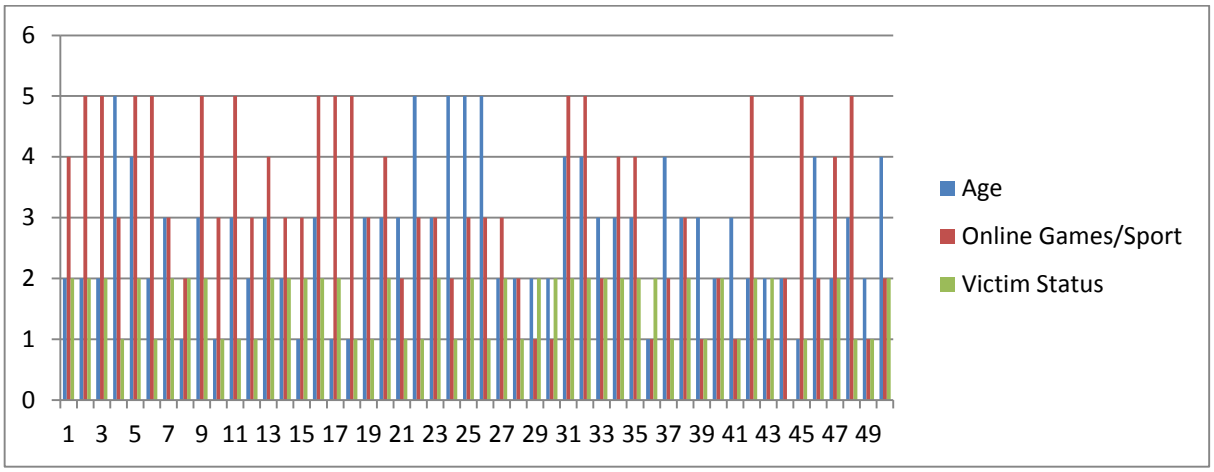


Figure 4. Above depicts the relationship between students that are actively involved in accessing social media frequently, and for what purpose they use it for, either academic research while online or pornography related reasons. The results revealed that Students within the age of 15-18(3) get involve in social media access while online all the time for crime related offense and seldom get involve in academic research, while student within the age of 19-22(4-5) follow suite with less attention for academic research. However, it is observed that some Students within the age of 16-22(3-4-5) get seldom involve in academic research, probably because students within this age group are assumed or expected to be at their final year (S.S.3), or have finished secondary school seeking

for an A Level admission into a higher institution which may be one of their compelling force for academic research.



.

Figure 5. Above depicts the relationship between age, online games/sport and victims of cybercrime. The study revealed that students within the age of 15-18(3) get mostly involve in online games and are the most victims of cybercrimes while students within the age of 10-14(1-2) are less victims since they seldom use mobile phones. However, we observed that, as their age advances their crime rates as well as victimization rate increases.

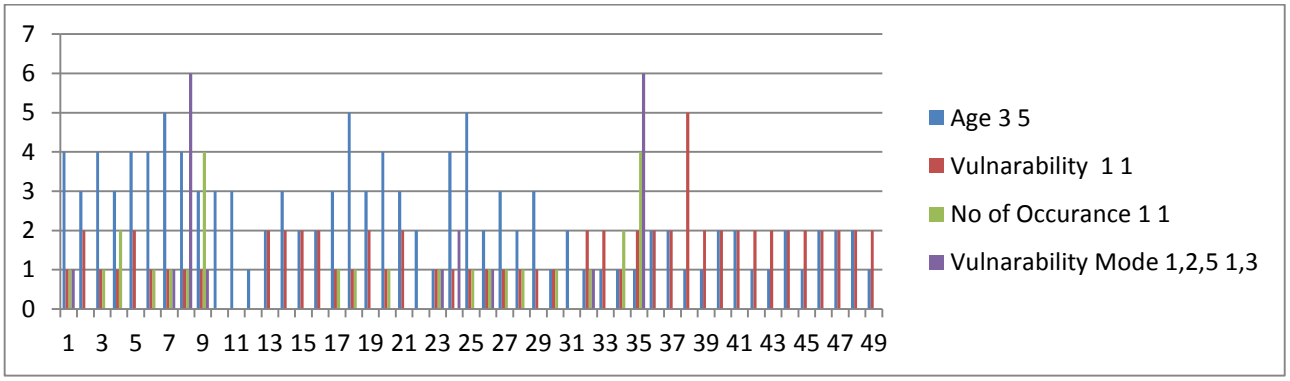


Figure 6. Above depicts the relationship between age, number of occurrence of cybercrime and vulnerability mode. The study showed that Students within the age of 15-18 and above (3) are most affected as victim of cybercrime and more vulnerable while the students within the age of 10-14(1-2) Seldom get involve in cybercrime. However, we observed that as their various age advances their crime rates also increase. That is they become more victimize of cybercrime as well as more active in cyber related crime.

5.1 Definition, Meaning and Interpretation of Results

This section present a discussion and explanation of some terms and definition of content, the graphs are discussed from table one to five as seen bellow.

IN TABLE 1 BELOW ARE THE DEFINATION OF TERMS AND MEANING FOR FIGURE 1. ABOVE		
Definition of Terms	**Description**	**Meaning**
Age	1, 2, 3,4,5	This are the five age represented as (1= age between 10-12), (2=12-14), (3=15-18), (4=19-21), (5=22 above)
Gender	1 or 2	1 represents male while 2 represent female
Marital Status	1 or 2	1 represent single while 2 represent married

IN TABLE 2: BELOW ARE THE DEFINATION OF TERMS AND MEANING FOR FIGURE 2. ABOVE		
Definition of Terms	**Description**	**Meaning**
Age	1, 2, 3,4,5	This are the five age represented (1= age between 10-12), (2=12-14), (3=15-18), (4=19-21), (5=22 above)
Internet Access	1,2,3,4,5	1=all the time, 2= most times, 3=sometimes, 4= seldom, 5=never

Proficiency	1,2,3,4,5	1=Excellent, 2=Very Good, 3=Good, 4=Average, 5=Poor

IN TABLE 3: BELOW ARE THE DEFINATION OF TERMS AND MEANING FOR FIGURE 3. ABOVE		
Definition of Terms	**Description**	**Meaning**
Age	1, 2, 3,4,5	This are the five age represented as (1= age between 10-12), (2=12-14), (3=15-18), (4=19-21), (5=22 above)
Sos Media Account	1,2,3,4,5	1=Facebook, 2= WhatsApp, 3=Instagram, 4= YouTube, 5=None
Pornography	1,2,3,4,5	1=all the time, 2= most times, 3=sometimes, 4= seldom, 5=Never

IN TABLE 4: BELOW ARE THE DEFINATION OF TERMS AND MEANING FOR FIGURE 4. ABOVE		
Definition of Terms	**Description**	**Meaning**
Age	1, 2, 3,4,5	This are the five age represented as (1= age between 10-12), (2=12-14), (3=15-18), (4=19-21), (5=22 above)
Sos Media Involvement	1,2,3,4,5	1=all the time, 2= most times, 3=sometimes, 4= seldom, 5=Never
Academic Research	1,2,3,4,5	1=all the time, 2= most times, 3=sometimes, 4= seldom, 5=Never

IN TABLE 5: BELOW ARE THE DEFINATION OF TERMS AND MEANING FOR FIGURE 5. ABOVE		
Definition of Terms	**Description**	**Meaning**
Age	1, 2, 3,4,5	This are the five age represented as (1= age between 10-12), (2=12-14), (3=15-18), (4=19-21), (5=22 above)
Online Game/Sport	1,2,3,4,5	1=all the time, 2= most times, 3=sometimes, 4= seldom, 5=Never
Victim of Cybercrime	1 or 2	1=Yes, 2=No

IN TABLE 6: BELOW ARE THE DEFINATION OF TERMS AND MEANING FOR FIGURE 6. ABOVE		
Definition of Terms	**Description**	**Meaning**
Age	1, 2, 3,4,5	This are the five age represented as (1= age between 10-12), (2=12-14), (3=15-18), (4=19-21), (5=22 above)
No of occurrence as Victim of Cybercrim	1,2,3,4,5	1=1-5times, 2= 6-10times, 3=11-15times, 4=16-20times, 5=20times above
Vulnerability Mode	1,2,3,4,5,6,7	1=Fake SMS, 2=Advance Fee Fraud, 3=Money Theft through ATM, 4=Piracy, 5=Forgery,6=Spamming, 7=others

6.0 Conclusion and future work

This section concludes our research study and presents open issues for further research work

6.1 Conclusion

In this paper, we presents Cybercrime, a threat to a moral Society: A Case study of Secondary School Students in Nigeria. The study highlights ways to mitigate the worrying growing rate of cybercrime carried out in some key sectors in Nigeria, especially our Secondary School institutions and presents a brief examination of these crimes in tertiary institutions within Kebbi and Sokoto State, and highlights methods of Cybercrime prevention in order to effectively combat cybercrimes in Nigeria.

6.2 Future Work

In our future work, we will present measures to efficiently combat cybercrimes.

References

[1] Lakshmi P. and Ishwarya M. (2015), *Cyber Crime: Prevention & Detection*,"International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).

[2] Hassan, A. B. Lass F. D. and Makinde J. (2012) *Cybercrime in Nigeria: Causes, Effects and the Way Out*, ARPN Journal of Science and Technology,VOL. 2(7), 626 – 631.

[3] Maitanmi, O. Ogunlere, S. andAyinde S. (2013), *Impact of Cyber Crimes on Nigerian Economy*, The International Journal of Engineering and Scienc (IJES, vol. vol 2(4), 45–51.

[4] Ewepu G, (2016) *Nigeria loses N127bn annually to cyber-crime* — NSA bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

[5] Shandilya A. (2011) *Online Banking: Security Issues for Online*

payment,from www.buzzle.com/articles.
[6] Parthiban L. and Raghavan A. R. (2014), *The effect of cybercrime on a Bank's finances*, International journal of Current Research and Academic Review, vol. 2(2), no. 173–178, Retrieved Feb. 2014 from www.ijcrar.com
[7] MichaelA.,Boniface., A. and Olumide, A. (2014) *Mitigating Cybercrime and Online Social Networks Threats in Nigeria*, Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz, vol. Vol I WCECS 2014, 22–24.
[8] Okeshola F.B. and 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, vol. 3(9), 98-114.
[9] Ndible N., (2016*) Practical Application of Cyber Crime* Issues Retrieved on May 6, 2016
[10] Moses A. Agana and Hight C. Inyiama (2015), Cyber Crime Detection and Control Using the Cyber User Identification Model, *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS 2249-9555 Vol. 5, No5, October 2015*
[11] Suleman Ibrahim (2016), Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals, International Journal of Law Crime and Justice 47 (2016) 44e57
[12] Marthie Grobler, Joey Jansen van Vuuren and Jannie Zaaiman (2013), Preparing South Africa for Cyber Crime and Cyber Defense, Systemics, Cybernetics and Informatics Volume 11 - Number 7 - Year 2013 ISSN: 1690-4524
[13] Folashade B. Okeshola & Abimbola K. Adeta (2013), the Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria American International Journal of Contemporary Research Vol. 3 No. 9; September 2013
[14] Rola Al Halaseh Ja'far Alqatawna (2016), Analyzing CyberCrimes Strategies: The Case of Phishing Attack, 978-1-5090-2657-9/16 $31.00 © 2016 IEEE
[15] Kazeem Abimbola Adeta (2014), Pattern and Consequences of Cyber-Crime in Tertiary Institutions in Zaria, JUNE, 2014
[16] Mike Redford (2011), JD (Criminal Law), LL.M (Anti-Money Laundering & E-Commerce Law), European Intelligence and Security Informatics Conference, 978-0-7695-4406-9/11 $26.00 © 2011 IEEE
[17] Wada & Odulaja (2012), Electronic Banking and Cyber Crime in Nigeria - A Theoretical Policy Perspective on Causation, Afr J. of Comp & ICTs. Vol 5. No. 1. pp 69-82.
[18] Chibuko Raphael Ibekwe (2015), The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions, PhD Thesis JULY 2015 of Informing Science & IT Education Conference (InSITE) 2015
[19] B. A. Omodunbi, P. O. Odiase, O. M Olaniyan and A. O. Esan (2016), Cybercrimes in Nigeria: Analysis, Detection and Prevention, Journal of Engineering and Technology, Volume 1, Issue 1, September 2016, 2579-0617
[20] Wada F. and Odulaja G. O. (2014), "Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation," Afr J Comp & ICT, Vol 4(3), no. Issue 2. 2016.
[21] A Summary of the Legislation on Cybercrime in Nigeria, Legislative & Government Relations Unit, Public Affairs Deparment,Federal Bureau of Investigation (2016), ATM skimming,Retrieved June 8, 2016.
[22] Iroegbu, *E "Cyber-security: Nigeria loses over N127bn annually through Cybercrime,"* Jun. 9, 2016.