IEEE Compter Society – Nigeria - Technical Paper Series

DOI: dx.doi.org/10.22624/iSTEAMS/V26P10-IEEE-NG-TS
CrossREF Member Listing - https://www.crossref.org/06members/50go-

An Empirical Analysis of Cybercrime Trends and Its Impact on Moral Decadence Among Secondary School Level Students in Nigeria

M. A. Ahmad
Department of Computer Science
Kaduna State University
Kaduna, Nigeria
muhdaminu@kasu.edu.ng
+2348066256878

D. D. Wisdom
Department of Mathematics
Usmanu Danfodiyo University
Sokoto, Nigeria.
danieldaudawisdom1@gmail.com
+2347030743902

S. Isaac
Dept of Computer Science
Kaduna State University
Kaduna, Nigeria.
samson.isaac@kasu.edu.ng
+2348035370205

Abstract: ***Cybercrimes in various forms are on the raise daily; these crimes pose a potential threat to our moral society as well as economy and nation building at large. They are namely: social engineering, malvertising, ransom ware, Spamming, Botnets, fake bank alert messages (SMS) /unsolicited SMS requesting you to provide bank details as Bank Verification Number (BVN), fraud, identity theft, piracy, pornography, hacking, fraudulent e-mail related SMS, forgery such as fake documents as Certificate etc. Thus, Cybercrime is gradually becoming a threat to our moral society at large. Hence, the increase number of cybercrime rate is an open field of ongoing research studies. Therefore, we have proposed a new approach that emphases on the prominent cybercrimes carried out around the world, and presents a precise study in Nigeria within some secondary school students. The study revealed a new approach to fighting Cybercrimes in order to combat cybercriminals.***

Keywords: *Cybercrime, Botnets, Malvertising, Ransom ware, Pornography.*

I. INTRODUCTION AND BACKGROUND

Cybercrimes are on the raise daily in various forms; these crimes pose a potential threat to our moral society, economy and nation building at large. A moral society is a pedestal for technology and social development. While the trend of technology increases threats as cybercrime are major setbacks as well. Since Cybercrime or Cyber related Crimes are equally on the raise with much severe effect on the community at various levels [3].

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 had the highest cyber-attacks of 35.4% and 12.8% respectively, according to [1] 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, spamming etc [3]. Cyber-crime evolves from wrong application/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 [2]. 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.

A. Basic Concept of Cybercrime

Cybercrime is an emerging trend that is gradually growing as the internet continues to penetrate all sectors in our societies 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, viruses as malware etc [4]
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).

B. Causes of Cybercrimes in Nigeria

The following are some of the few newly identified causes of cybercrimes [5].

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 or source of livelihood.
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 (PC). Some personal computers do not have proper or competent security control. Therefore, 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 most 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.

C. 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 [5].

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. Although 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. As more cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its previous ones respectively.

II. BANKING SECTORS

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 [6]. As the security level in this sector becom
es 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 [7]. and sabotaging data in computer networks of organizations.

A. 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, implemented in the year 2015 by the Central Bank of Nigeria, as instructed by the current sitting President Mohammadu Buhari 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.

B. Social Engineering

Social engineering is a technique used, where cybercriminals make a direct contact with individuals through phone calls, emails, or even in person. Mostly, they try to act like legitimate Persons. They will best friend individuals in order to gain trust until you provide your important information and personal data to them.

C. Malvertising

Malvertising is a technique of filling websites with advertisements carrying malicious codes. Where users will click these advertisements, thinking they are legitimate. Once they click these ads, they will be redirected to fake websites or a file carrying viruses and malware which will repeatedly be downloaded.

D. Cyber stalking

Cyberstalking is an approach that includes following an individual online secretly. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyberstalking are women and children being followed by men and pedophiles.

E. Piracy

The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally replicated.

F. Cyber bullying

Cyber bullying is one of the widespread crimes on the raise globally. It is a form of victimization carried over to the internet. Globally leaders are aware of this crime and have pass laws and acts that may further prohibit the proliferation of the criminal acts, yet this is still a growing concern.

G. Spamming

Spamming uses electronic messaging systems, most commonly emails in sending messages that host malware, fake links of websites, and other malicious programs. Email spamming is very popular. Unsolicited bulk messages from unfamiliar organizations, companies, and groups are sent to large numbers of users. It offers deals, promos, and other attractive components to deceive users, in which users usually fall pray.

H. Phishing

Phishing is another dynamic approach such that cybercriminals act like legitimate individuals or organization. They use “email spoofing” to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

I. Hacking

Hacking includes the partial or total acquisition of certain functions within a system, network, or website. This also aims at accessing important data and information, breaching privacy. Most “hackers” attack corporate and government accounts. There are different types of hacking means and procedures.

J. Identity Theft

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

III. SCAMMING

Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of money or cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

A. Computer Viruses

Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy

computers, networks, and systems. Viruses can spread through removable devices and the internet.

B. Ransom-ware

Ransom-ware is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransomware. In 2017, over $5 billion is lost due to global ransomware.

C. DoS Attack

Denial of Service attack (DoS) is one of the most popular means of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DoS attack, giving hackers the chance to hack the system. And do away with some vital information or damage them completely.

D. Botnets

Botnets are controlled by remote attackers called "bot herders" in order to attack computers by sending spams or malware. They usually attack businesses and governments as botnets specifically attack the information technology infrastructure. There are botnet removal tools available on the web to detect and block botnets from entering your system (s).

E. Fraud

Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair profits.

F. Banking Fraud

Hackers target the vulnerability ties in the security of various bank systems and transfer money from uncountable accounts to their personal accounts. 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 running into millions of naira unlawfully.

IV. 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 Electronic commerce websites, where the hackers' makes used of a cloned website to perpetrates their crimes for their own profits.

A. *Data and Airtime theft*

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.

B. 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 also 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.

C. 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, causing harm to individuals, especially the youth.

D. Child Pornography

Mostly, this cybercrime involves the exploitation of children in the porn industry. Child pornography is a $3-billion-a-year industry. Unfortunately, over 10,000 internet locations provide access to child porn. However, some countries have provided laws that now penalize child pornography. Yet this has now however resulted to a very high level of moral decadence in our society today.

E. 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.

This is done whenever a customer uses the machine (FBI, 2011). Unknown to users. Also, another cybercrime carried out via this means in Nigeria includes internet order fraud. Internet other fraudster involves inputting stolen cards numbers on online comer in order to exploit innocent people.

F. 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].

V. 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.

A. 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.

B. 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.

C. Email inspection

The idea of 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 respectively.

VI. 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 Con-figuration 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 [8]. 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.

A. 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][8].

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 as namely: 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. Individual proper Security Controls

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, Facebook page, or 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 it is always safer to go directly to the website of the retailer.

VII. CYBERCRIMES IN SECONDARY SCHOOLS

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 student's tries to shield their real self's 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, table 1 to 5. Each question has an option while others are multiple choice Questions.

A. 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 [9]. Cyber Crime Detection and Control Using the Cyber User Identification Model was proposed 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 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 identify and record the geographical location of each user, the MAC address of the system used, the date, 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 [10]. 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 [11].

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.

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 addresses the 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 [12]. Causes of Socioeconomic Cybercrime in Nigeria was proposed 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 [13]. Analyzing Cybercrimes Strategies: The Case of Phishing Attack was proposed 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 [14]. U.S. And EU Legislation on Cybercrime was proposed 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 [15][16]. Electronic Banking and Cyber Crime in Nigeria a Theoretical Policy Perspective on Causation was proposed 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.

VIII. 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 to question 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.

IX. 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.

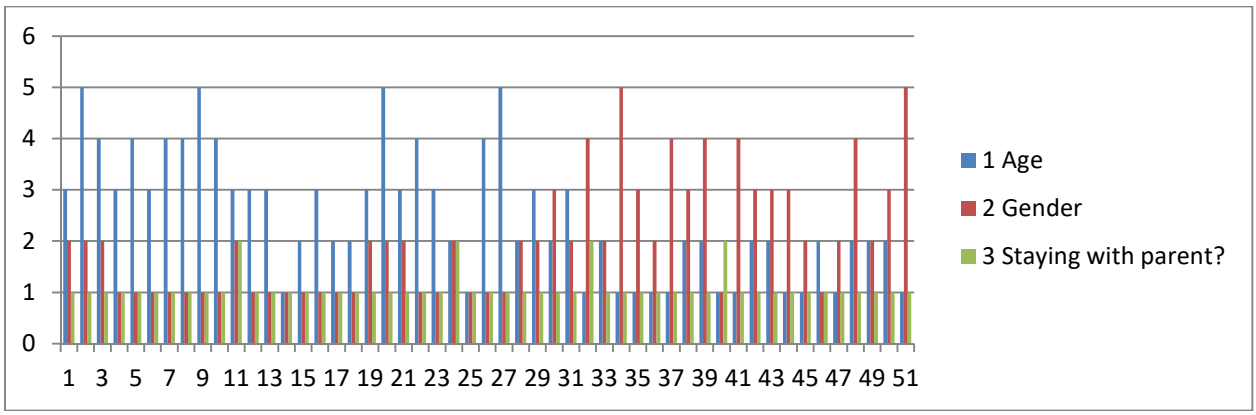

Fig. 1: Above shows the relationship between Age, Gender and students who stay with their parents and likewise those that stays away from their parents.

Figure 1 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.

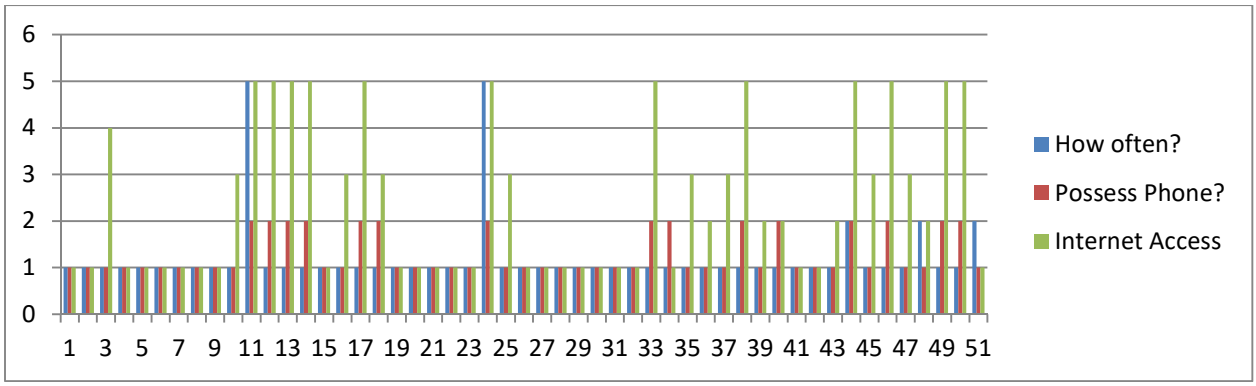

Fig. 2: Relationship between how often student's stays with their parents, how many of them possess mobile phone

Figure 2 depicts the relationship between how often student's 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.

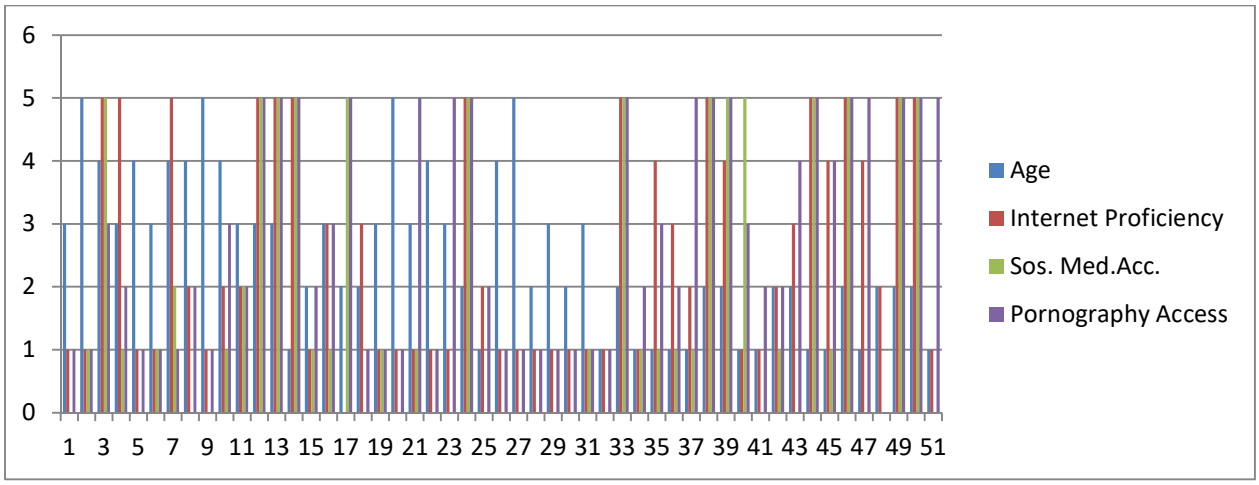

Fig. 3: Above depicts the relationship between age, how many social media accounts a student has, and how often they visit sites related to pornography

Fig. 3 depicts the relationship between age, how many social media accounts a student has, and how often they visit 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 thus supporting the findings in [17]. .

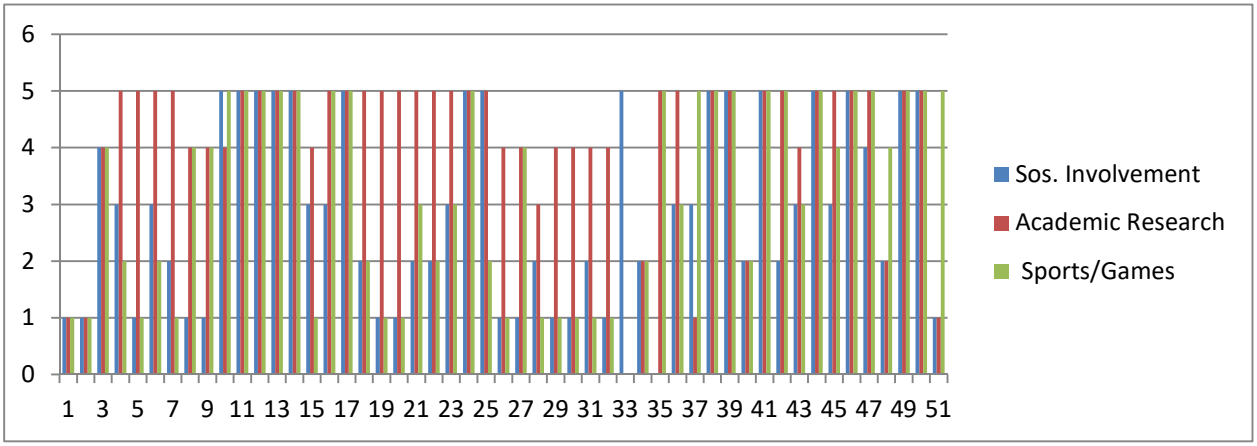

Fig. 4: Above depicts the relationship between students that are actively involved in accessing social media frequently,

Fig. 4 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.

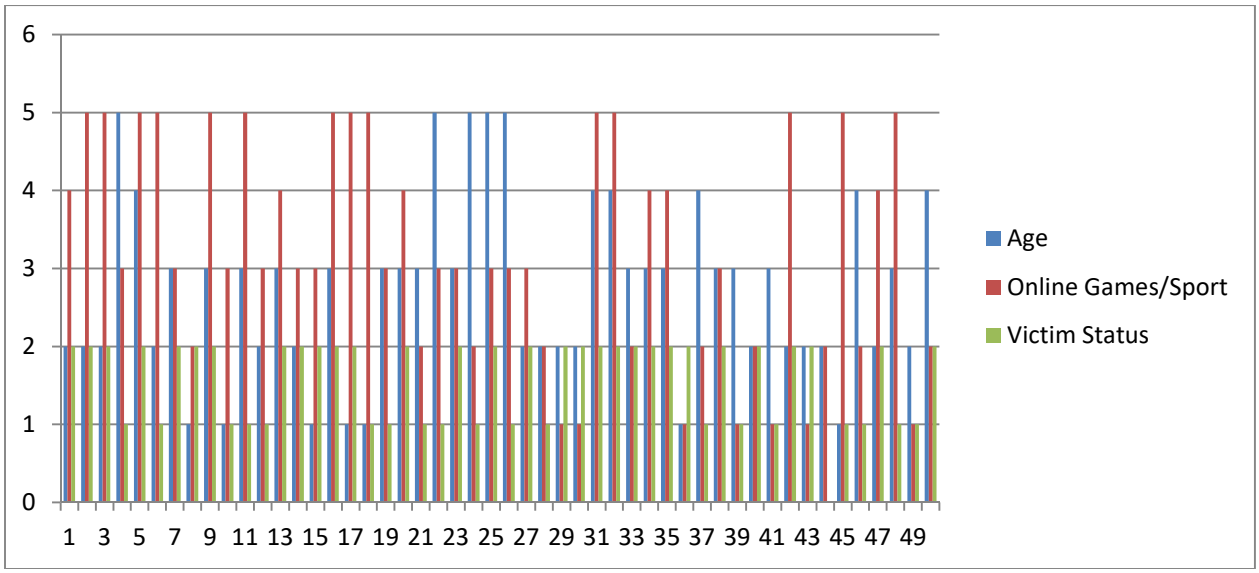

Fig. 5: Above depicts the relationship between age, online games/sport and victims of cybercrime

Fig. 5 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.

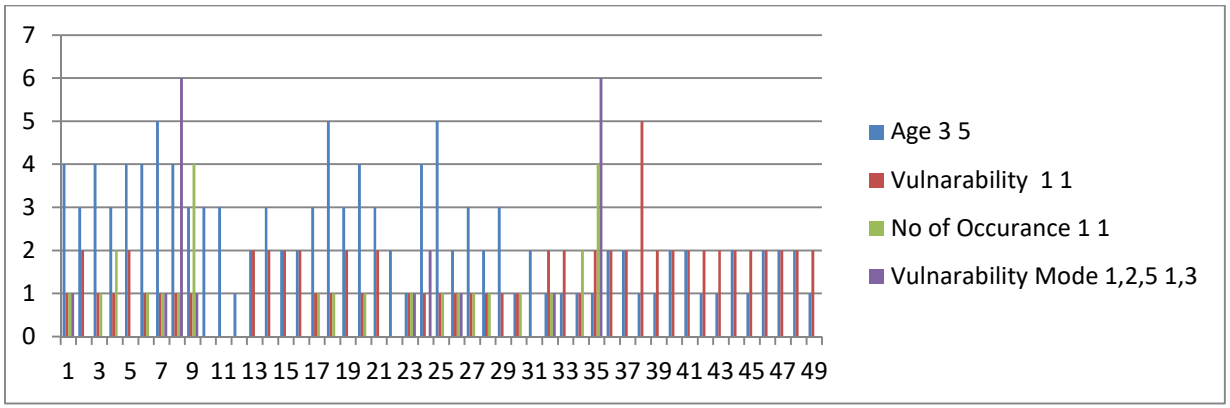

Fig. 6: Above depicts the relationship between age, number of occurrences of cybercrime and vulnerability mode.

Fig. 6: Above depicts the relationship between age, number of occurrences 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.

A. Definition, Meaning and Interpretation of Results

This section presents a discussion and explanation of some terms and definition of content, the graphs are discussed from table one (1) to five (5) as seen bellow.

Table 1: Definition of Terms and Meaning for Figure 1.		
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

Table 2: Definition of Terms and Meaning for Figure 2.		
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

Table 3: Definition of Terms and Meaning for Figure 3.		
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

Table 4: The Definition of Terms and Meaning for Figure 4.		
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

Table 5: The Definition of Terms and Meaning for Figure 5.		
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

Table 6: The Defination of Terms and Meaning for Figure 6.		
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

X. CONCLUSION

This paper presents the prevailing challenges experience in our society today, due to the growing reliance and importance of the internet. The paper studied the presents rise in moral decadence due to cybercrime using the average youth in secondary schools as case study in Nigeria. Finally, the study also highlights ways to mitigate the worrisome growing rate of cybercrime carried out in some key sectors in Nigeria, especially the Secondary School institutions and presents a brief examination of these crimes in some secondary schools within Kebbi and Sokoto State, and proposed methods of cybercrime prevention to effectively combat cybercrime rate in the educational sector.

REFERENCES

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

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

[3] Maitanmi, O. Ogunlere, S.and Ayinde, S. "*Impact of Cyber Crimes on Nigerian Economy"*, International Journal of Engineering and Science (IJES), 2013. V 2(4). PP 45–51.

[4] Wada, F. and Odulaja, G. O. "Electronic Banking and Cyber Crime in Nigeria" – *A Theoretical Policy Perspective on Causation,* Afr J Comp & ICT, Vol 4(3), no. Issue 2. 2016.

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

[6] Shandilya, A. "*Online Banking": Security Issues for Online payment*, from 2011. www.buzzle.com/articles.

[7] Parthiban, L. and Raghavan, A.R. "*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

[8] Michael, A. Boniface, A. and Olumide, A. "Mitigating Cybercrime and Online Social Network Threats in Nigeria", *Proceedings of the World Congress on Eng and Computer Science,* Vol.1 (WCECS 2014), PP 22–24.

[9] Okeshola, F.B. and A.K Adeta ."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), pp 98-114.

[10] Ndible, N. "*Practical Application of Cyber Crime"* Retrieved May 6, 2016.

[11] Moses, A.A and Hight, C. I. "Cyber Crime Detection and Control Using the Cyber User Identification Model, *IRACST" -International Journal of Computer Science and Information Technology & Security Vol. 5, No5, October, 2015.*

[12] Suleiman, I. "Social and contextual taxonomy of cybercrime": Socioeconomic theory of Nigerian cybercriminals, *International Journal of Law Crime and Justice* 47 2016.

[13] Marthie, G. V Joey J-V and Jannie, Z. "Preparing South Africa for Cyber Crime and Cyber Defense", *Systemics, Cybernetics and Informatics* Vol.11 - NO 7. 2013.

[14] Adeta, K. A. and Pattern, K. A. "Consequences f Cyber-Crime in Tertiary Institutions in Zaria", JUNE, 2014.

[15] Ibekwe, C. R "The Legal Aspects of Cybercrime in Nigeria": An Analysis with the UK Provisions, InSITE 2015.

[16] Halaseh, R. A-l and Alqatawna, J. "Analyzing Cybercrimes Strategies": The Case of Phishing Attack, 978-1-5090-2657-9/16 $31.00 © 2016 *IEEE.*

[17] Longe, O.B., Chiemeke, S.C, Onifade, O.F., Balogun, F. M., Longe, F.A. & Otti, V.U. (2007). Exposure of Children and Teenagers To Internet Pornography In South Western Nigeria – Concerns, Trends & Implications. Journal of Information Technology Impact. Vol 7, No. 3.