

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 5 ISSUE : 4 Print / Issue Publication Date: 15-Oct-2020

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2020.v05i04.015

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117
Published Online August 2020 in IJEAST (http://www.ijeast.com)

COMBATTING CYBERCRIMES IN THE EDUCATION SECTOR

Daniel Dauda Wisdom
Department of Mathematics, Computer Unit, Usmanu Danfodiyo University Sokoto(UDUS), Sokoto State, Nigeria

Adamu Bashir Ismail
Departments of Computer Science, Umar Ali Shinkafi Polytechnic Sokoto, Sokoto State, Nigeria

Abdullahi Bashar Abubakar
Department of Computer Science Umar Ali Shinkafi Polytechnic Sokoto, Sokoto State Nigeria

Mairiga Bawa Ribah
Faculty of Science Education Ahmadu Bello University (ABU) Zaria, Nigeria.

Ebenezer Akinyemi Ajayi
Faculty of Computing and Information, Multimedia University, Melaka, Malaysia.

Danjumma Bedi
Department of Mathmatics, Computer Unit,Usmanu Danfodiyo University Sokoto, Sokoto State

ABSTRACT - Several computer related crimes known as cybercrimes are committed daily such as fake bank alert messages (SMS)/unsolicited SMS requesting details as Bank Verification Number (BVN), Advance fee fraud (Yahoo Yahoo), identity theft, piracy, pornography, hacking, forgery such as fake certificates etc. Thus, People connected to the internet through their computers/mobile phones have experienced such crimes. Therefore, the increasing rate of cybercrimes in our societies today, is a critical concern and an imperative area of research study. Hence, the impact of these crimes can be felt severely on a nation and it economy at large. We have propose a new approach that focuses on the prominent cybercrimes in Nigeria and presents a brief analysis of cybercrimes within the Nigerian tertiary institutions. And finally highlights methods of Cybercrime detection and prevention in order to efficiently combat cybercrimes.

Keywords: Cybercrime, Identity theft, Hacking, Pornography.

I. INTRODUCTION AND BACKGROUND

One of the fastest emerging epidemics worldwide is Cybercrime (CC) as technological trend advances, so also the rate of CC increases. The world would have been a better place with ample opportunities due to an ever increase rate in technology and ICT related developments. However CC 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 CC. The 21st Century generation therefore most take insightful and purposeful decision so as to combat these menace called CC. 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 2006/2015, 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][20]. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the youth; more especially in higher institution [15][24][26]. Cybercrime is defined as type of crime committed by criminals who make use of a computer devices as tools and the internet as a connection in order to reach a variety of objectives, as illegal downloading of music, files and videos, etc. [3][10]. Cyber-crime evolves from the wrong application such as abuse of internet services and so on.

1.1 Basic Concept of Cybercrimes

Cybercrime is an emerging trend that is gradually growing as the internet continues to penetrate every sector of our society and the future is yet unknown. Cybercrime may be divided into two categories [18]:

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, Money theft through the ATM, SMS requesting you to provide bank details as BVN.

1.2 Causes of Cybercrimes in Nigeria

The following are some of the few newly identified causes of cybercrimes [2][30].

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 [30].

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 [30].

3. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime. Thus, 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 [14].

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

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, Life 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.

5. Age: It's observed from our research study using our fact finding Questioners that age significantly has an influence on an average youth in their involvement in cybercrime.

1.3 Various 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 higher rate. As the internet grows to become more accessible and more facilities become reliant on it for their daily operation, likewise the rise in 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. Recently the United States of America (US) apprehended 6 Nigerians (18/06/2020) in the US for cyber related crime as published by the Nigerian new publishers. 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 [11] [22].

1.4 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/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.

1.5 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.

1.6 Phishing

Phishing is a theft of 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 [21][27]. In Phishing mail messages, the fraudsters' tries to find a way to convince and gain the trust of users. Phishing mails are mostly carried out on bank customers either through mail, text Messages or phone call requesting individual bank information for the purpose of criminal activity. In some cases social media platforms like what-Sapp, Facebook, etc are used to initiate communication just to establish trust and confidence, there by exploiting individuals for the said motive subsequently [21].

1.6.1 Cyber-theft / Banking Fraud

Hackers target the vulnerability-ties in the security of various bank systems and transfer money from

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117
Published Online August 2020 in IJEAST (http://www.ijeast.com)

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 usually treated as legitimates deductions unknown.

1.6.2 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 fake 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.

1.6.3 Education Sector and Cybercrime
The educational sector in Nigeria suffers greatly from electronic crimes which are perpetuated mostly by students in tertiary institutions (Universities, Polytechnic and monotechnic and others).

1.6.4 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.

1.6.5 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 and the entire societal moral decadence as well.

1.6.6 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 platforms in order to access money illegally.

1.6.8 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].

1.6.9 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 unknown.

1.7 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 while relating with the said victims.

1.7.2 Personal Social Site-Hijacking
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 [8].

II. WAYS TO DETECT CYBERCRIMES

The following are some of the ways by which cybercrimes can be detected

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. While this may not be the

only trick, a genuine address should contain https. The s stands for protected (secured); otherwise any address with no s attached to the http is likely to be cybercriminal sites and should be treated as such.

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 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 [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 Measures to Prevent 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 [20] [23]. However, 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 rates, and increase customers.
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 Analyses of Cybercrimes
The aim of this analysis 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 selected tertiary institutions in Sokoto-state. The research questions were distributed in the Usmanu Danfodiyo University, Sokoto, Sokoto State (UDUS) and some selected student areas within the sokoto state metropolis; however, our study covers a total of 50 students Questionnaire with an average age range between 15 to 31 years above. The prestigious Usmanu Danfodiyo University been the oldest and the most populated tertiary institution within the sokoto state metropolis was our key focus in this study, The questionnaire consisted of 14 questions that cuts across all aspects of cybercrime in Nigeria especially within campuses. Each question has an option which could be precisely seen below in the appendix: From the options below, each student were to select one for every question given, except for Questions **7** and **14** where a student is allowed to select more than 1 option(s).

III. RELATED LITERATURES

This section presents a review of related literatures.
In [12], Cybercrimes Investigation and Intrusion Detection in Internet of Things According to Data Science Methods were propose to investigate and detect different type of attacks and invasion. This research introduces a principle of Digital Forensics, Intrusion Detection and Internet of Things as well as exploring data science concepts and methods that can help the digital investigators and security professionals to develop a data science techniques and methods that can be adapted to a unique context of Internet of

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117
Published Online August 2020 in IJEAST (http://www.ijeast.com)

Things environment for performing intrusion detection and digital investigation process in forensically sound and timely fashion manner.

In [13], Cybercrime Escalation Vs. solutions: a Literature Snapshot was propose to alert the society to claim attention in national capitals and dedicated legislation on cybercrime to supplement the Indian Penal Code. This research introduces an analytical approach from emergence of cybercrime to prevention strategies used for cybercrime. The study throws light on status of cybercrime in current scenario and presents available solutions including steps taken by non-government and government organizations to avoid cybercrime and forthcoming challenges
as well as measures on both the National, International agreement and solutions to deal with these same problems.

In [15], A Spiritual Dimension To Cybercrime in Nigeria: The 'yahoo Plus' Phenomenon propose that Cybercrime in Nigeria is largely perpetrated by young people and students in tertiary institutions, usually called the yahoo boys. They depend on their computer facility to victimize unsuspected persons in cyberspace. Another new phenomenon in cybercrime is mixing of spiritual elements with internet surfing to boost cybercrime success rates. In [16], incorporating the Human Element in Anticipatory and Dynamic Cyber Defense was proposed to identify five main study areas that requires quick response. Using a criminological framework and empirical evidence of observations as well as interviews done at Industrial Control Systems Computer
Emergency Response Team's (ICS-CERT) Red/Blue. The study offers recommendations for further research and the relevance of multidisciplinary collaboration. In [17], WhatsApp Network Forensics: Discovering the Communication Payloads behind Cybercriminals was propose to to examine cybercriminals through network forensics and sniffing Techniques. The findings can support LEAs in discovering criminal communication payloads and facilitating the effectiveness of modern call record analysis.

Nigeria. In [19], Analysing Issues of Cyber Threats in Nigeria was propose to examines the pattern of cyber threats and information security in line with the Nigerian approach to meeting these challenges in the 21st century. The results of the analysis from the Questionnaire administered revealed the major group of the public that are largely active in committing cybercrime.

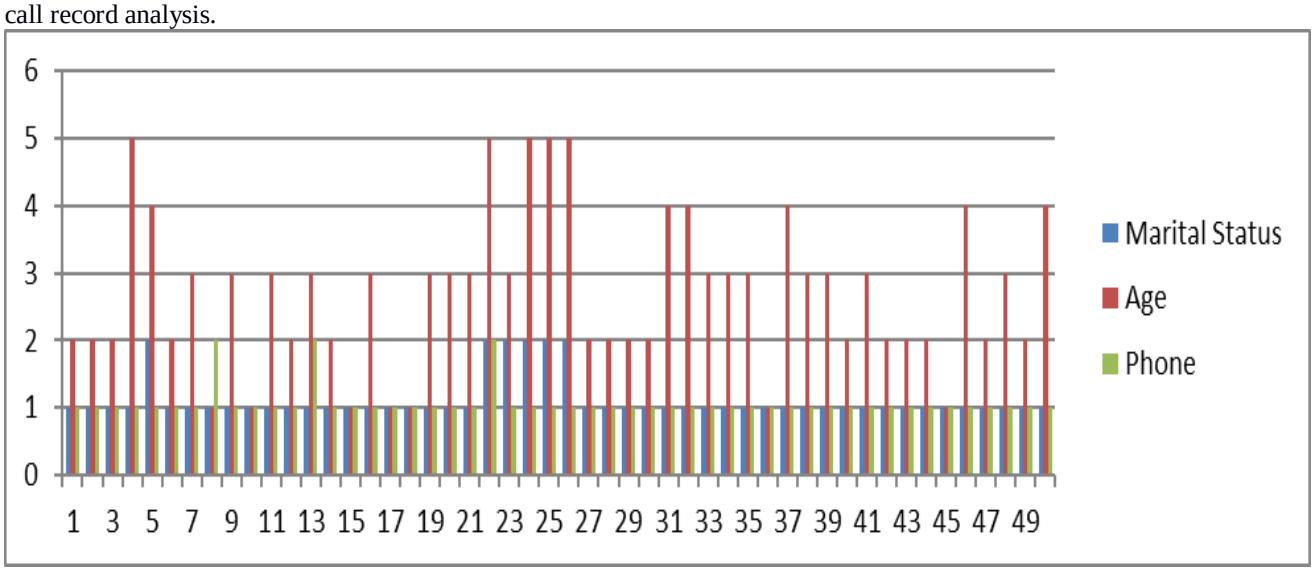
In [25], The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions was propose to provide insight into contemporary global cybercrime legislations and the shortfalls to their procedural enforcement. Analysize and present a critique to the provisions as provided in the recently enacted Nigerian Cybercrime (Prohibition and Prevention) Act 2015, in contradistinction to the existing legal framework in the United Kingdom and the other regional enactments like the Council of Europe Convention on Cybercrime, African Union Convention on Cyber security and Personal Data Protection 2014, as well as the ECOWAS Directive on Cybercrime.

IV. METHODOLOGY

The method employ for this research study was Questionnaire base. we developed a research Questionnaire that comprises of 14 fact finding questions and administered them mainly within the Usmanu Danfodiyo University, being the largest and the most populated tertiary institution within sokoto state metropolis, a sample of our Proposed Questionnaire is attached below in the appendix.

V. RESULT AND DISCUSSIONS

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



International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117
Published Online August 2020 in IJEAST (http://www.ijeast.com)

Figure1. Above shows the relationship between Age, mobile Phone and marital Status. The age depicts the different individual age range and its effect on the marital status as well as a mobile phone. The study revealed that youth within the age of 15-23 (1) Posses more mobile phones than the age group between 31 and above (2). And only few of them within the age of 19-23 are married which may pose a threat to cybercrime since they are not been saddle with responsibility yet, especially in environment like the sokoto state metropolis where marriage is given more consideration at early age.

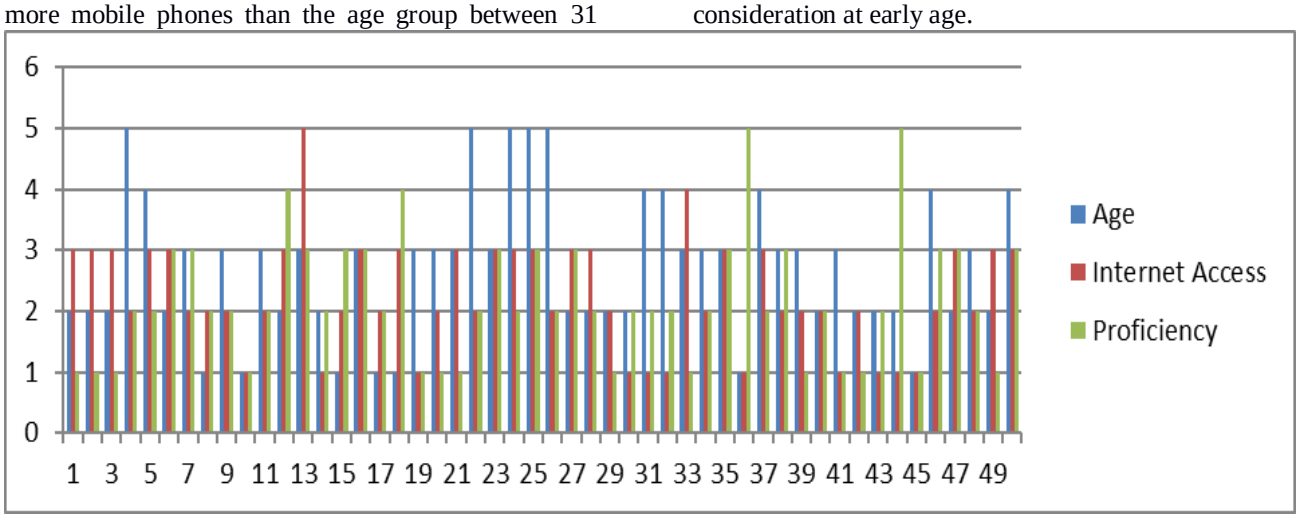


Figure2. Above depicts the relationship between age, how often students access the internet with their mobile phone and their proficiency on the use of the internet. The study above proves that student within the age of 15-18(1) access the internet all the time, while student within the age of 19-23(2). access the internet most times, and students within the age of 23-26(3) access the internet sometimes, and students within the age of 27-31above (4-5) access the internet seldom.

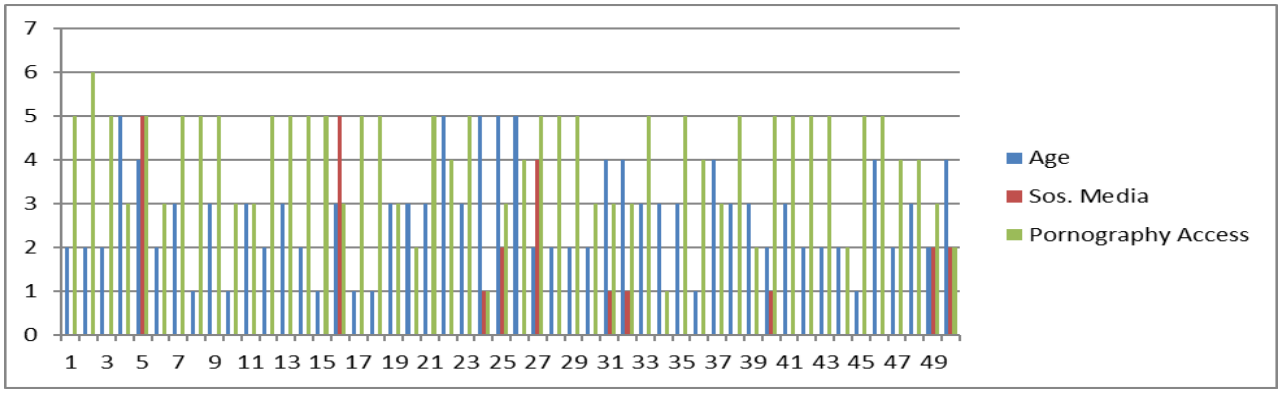


Figure3. Above depicts the relationship between age, how many social media accounts a students has, and how often they visits sites related to pornography. The study revealed that Students within the age of 15-18(1) has more social media accounts and are exposed to pornography access mostly, while students within the age of 19-22(2) follow suite. As they advance in age the rate of exposes to pornography decreases as well as number of social media accounts.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117
Published Online August 2020 in IJEAST (http://www.ijeast.com)

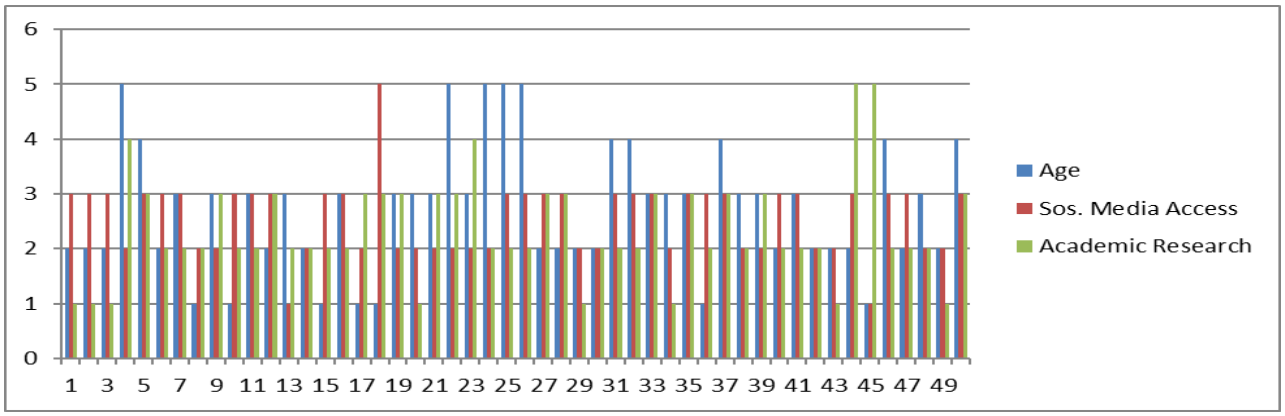


Figure4. Above depicts the relationship between age, how often students access social media while online, and use it for academic research while online. The results revealed that Students within the age of 15-18(1) get involve in social media access while online all the time for crime related offense and seldom get involve in academic research, while student within the age of 19-22(2) follow suite with little concern for academic research. However, Students within the age of 23-26(3) get more actively involve in academic research most times, properly because students within this age group are assumed or expected to be at their final year, which may be one of the reasons compelling them. This becomes a serious concern since students only become serious with their academic around the final year level which may be a reason for majority graduating with bad grades.

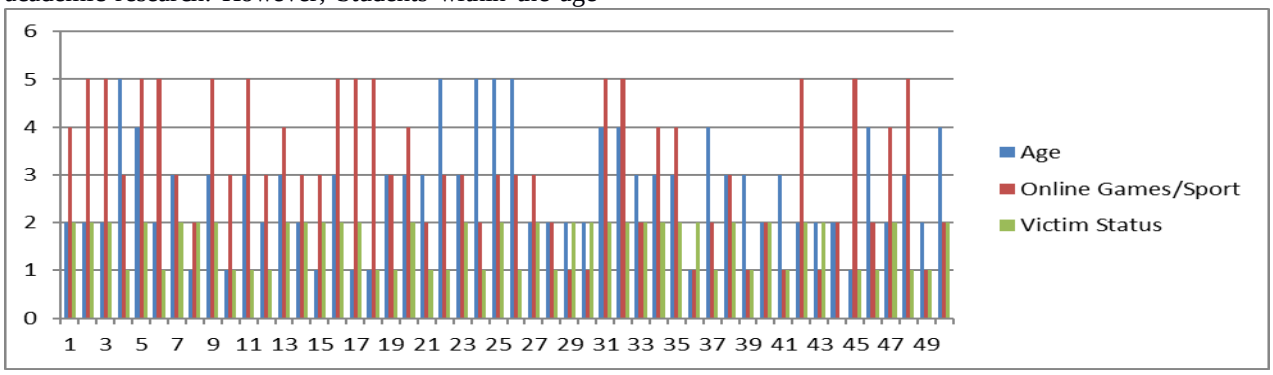


Figure5. Above depicts the relationship between age, online games/sport and victims of cybercrime. The study revealed that students within the age of 15-18(1) get mostly involve in online games and are the most Victims of cybercrime while students within the age of 19-22(2) follow suite. However students within the age of 23-26(3) are less involved and less victim of cybercrime likewise as the age advances.

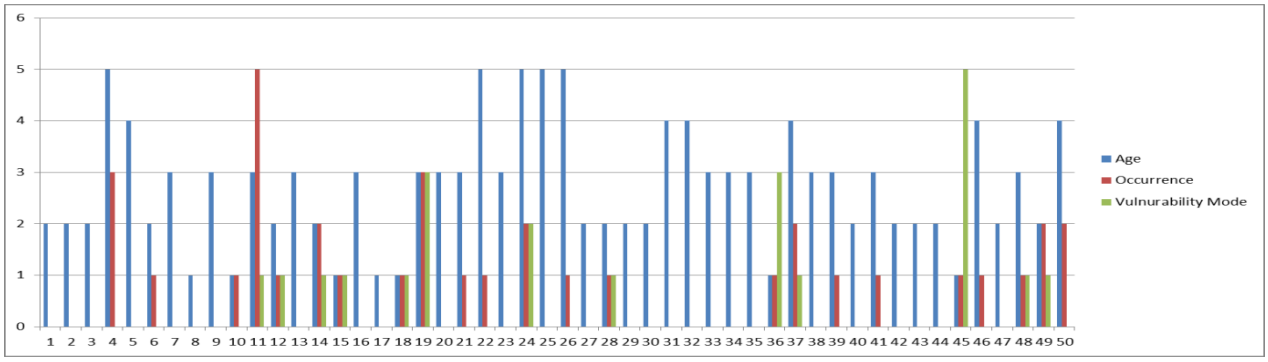


Figure6. Above depicts the relationship between age, number of occurrence of cybercrime and vulnerability mode. The study showed that Students within the age of 15-18(1) are most affected as victim of Cybercrime and more vulnerable while the students within the age of 19-22(2) follow suite. But, as their age advances they become less victims of cybercrime as well as vulnerability mode.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117
Published Online August 2020 in IJEAST (http://www.ijeast.com)

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 1 to 6 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 15-18), (2=19-22), (3=23-26), (4=27-30), (5=31 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 as (1= age between 15-18), (2=19-22), (3=23-26), (4=27-30), (5=31 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 15-18), (2=19-22), (3=23-26), (4=27-30), (5=31 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 15-18), (2=19-22), (3=23-26), (4=27-30), (5=31 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 15-18), (2=19-22), (3=23-26), (4=27-30), (5=31 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 15-18), (2=19-22), (3=23-26), (4=27-30), (5=31 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

VI. CONCLUSION

We have presented a new approach to prediction and easily understand the prevailing rate of cybercrime and its dynamics as well as methods that can be employed in order to decrease/eliminate the unwanted growing nature of cybercrime in Nigeria. In addition, the approach highlights ways to also minimize the worrisome growing rate of cybercrime carried out in some key sectors in Nigeria, especially our institutions and presents a brief analysis of these crimes in tertiary institutions in Nigeria. And finally revealed technics that will aid in curbing cybercrime effectively in Nigeria.

VII. 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 Science (IJES, vol. vol 2(4), 45–51.

[4] Ewepu G, (2016) *Nigeria loses N127bn annually-to-cyber-crime*-NSA, Availableat:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-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'sfinances*, International journal of Current Research and Academic Review, vol. 2(2), no. ISSN: 2347-3215, 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 availableat:http://ijma3.org/Admin/Additionals/Cybercrime/Nibal%20Idlebi%20

[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), ISSN: 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] Ezz El-Din Hemdan and D. H. Manjaiah (2018), Cybercrimes Investigation-and Intrusion Detection in Internet of Things Based on Data Science Methods, © Springer International Publishing AG 2018.

[13] Raksha Chouhan (2015), Cybercrime Escalation Vs solutions: a Literature Snapshot, Suresh Gyan Vihar University, Jaipur International Journal of-Converging Technologies and Management (IJCTM) Volume 1, Issue 2, 2015.

[14] 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

[15] Oludayo Tade (2013), A Spiritual Dimension to Cybercrime in Nigeria: The '*YAHOO PLUS*' Phenomenon, Institute for Research in Social Communication, Slovak Academy of Sciences 2013.

[16] Aunshul Rege (2016), Incorporating the Human Element in Anticipatory and Dynamic Cyber Defense Department of Criminal Justice Temple University Philadelphia, USA. 978-1-5090-6096-2/16/$31.00 ©2016 IEEE

[17] Fu-Ching TSAI, En-Cih CHANG, Da-Yu KAO (2018), WhatsApp Network, Forensics: Discovering the Communication Payloads behind Cybercriminals, ISBN 979-11-88428-01-4 ICACT2018 February 11 ~ 14, 2018

[18] 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

[19] Suleman Ibrahim Lazarus (2016), Causes of socioeconomic cybercrime in Nigeria, in Proceedings of the IEEE, November 2016

[20] 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

[21] Kazeem Abimbola Adeta (2014), Pattern and Consequences of Cyber-Crime in Tertiary Institutions in Zaria, JUNE, 2014

[22] 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

[23]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.

[24] Chibuko Raphael Ibekwe (2015), The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions, PhD Thesis JULY 2015

[25] O. K. Akinyokun, B. K. Alese, S. A. Oluwadare, O. Iyare, and G. B. Iwasokun (2015), Contributory Indices to Cybercrime Activities in Nigeria, Proceedings-of Informing Science & IT Education Conference (InSITE) 2015

[26] 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.

[27] 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.

[28] 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.
[29] Iroegbu, *E "Cyber-security: Nigeria loses over N127bn annually through Cybercrime,"* available at: http://www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/ Retrieved Jun. 9, 2016.
[30] Omodunbi, B. A, Odiase, P. O. Olaniyan O. M and Esan A. O: Cybercrimes in Nigeria: Analysis, Detection and Prevention, FUOYE Journal of Engineering and Technology, Volume 1, Issue 1, September 2016, 2579-0617 (Paper)

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

- Daniel Dauda Wisdom
- Adamu Bashir Ismail
- Abdullahi Bashar Abubakar
- Mairiga Bawa Ribah
- Ebenezer Akinyemi Ajayi
- Danjumma Bedi

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

JOURNAL METRICS

H-INDEX	i10-INDEX	IJEAST CITATIONS	PEER-REVIEWED & OPEN ACCESS
33	154	9,647 (IJEAST CITATIONS)	PUBLISHED MONTHLY

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

AUTHORS ARE OUR PRIORITY

We value our authors and recognize their contribution to the advancement of research and knowledge.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and professionals worldwide.

TIMELY PUBLICATION

We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

editor@ijeast.com
www.ijeast.com
India

2455-2143