International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2019.33658

Volume 5, Issue 12
December - 2019

Cybercrime, its Adherent Negative Effects on Nigerian Youths and the Society at Large: Possible Solutions

EBELOGU Christopher U[1], OJO Samuel D[2], ANDEH Chioma P[3], AGU Edward O[4]

Research Scholar[1-3], Lecturer[4]
[1-3]Department of Computer Science, University of Abuja, FCT Abuja, Nigeria
[4]Department of Computer Science, Federal University Wukari, Taraba State, Nigeria

ABSTRACT

Every country has its fair share of security challenges, but when the state of insecurity increases by the day, and then there is a need for urgent action. In Nigeria, the introduction of these three major inventions; the Computers, the Internet and the Mobile telephones gave rise to a huge outbreak of cybercrimes. It could be very evident that criminals and fraudsters leverage the anonymity supplied by means of the Internet to defraud unsuspecting victims. Unfortunately, the current social, economic and political trends have left a sour taste in the mouth of the youths; particularly, those from poor social and economic backgrounds. Notably, cybercrimes are of different categories in Nigeria ranging from; Internet frauds, software piracy, hacking, online scam, ATM or Credit card fraud, virus dissemination, phishing, cyber-stalking, and cyber-defamation. The occurrence of a high rate of unemployment, harsh economic conditions and bad educational systems also contributes immensely to the proliferation of cybercrimes in Nigeria. This paper analyses the adherent effects on the average Nigerian youth and the possible solutions. With Nigeria venturing into the cashless society, there is an urgent need to reduce the cybercrime menace ravaging our dear country.

Key Words: *Cybercrime, Cybercriminals, Phishing, Man-In-The-Middle (MITM), Cyber-stalking, Digital Fraud, Internet Fraudsters, Law Enforcement Agencies.*

1. INTRODUCTION

Cybercrime is a crime which involves the use of digital technologies in commission of offence, directed to computing and communication technologies. The modern techniques that are proliferating towards the use of internet activity results in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offence through illegal activity. The activity involves like attacking on Information center Data System, theft, child pornography built images, online transaction fraud, internet sale fraud and also deployment in internet malicious activities such as virus, worm and third party abuse like phishing, email scams etc. The universal approach of network like internet at all levels of network needs to recover from committing illegal activity in all over the world and to stop the criminal nature by protecting unlawful activity by enforcing different level of firewall setting within its offline control for every nation in order to monitor and prevent crimes carried out in cyberspace. Network security controls are used to prevent the access of hackers in networks which includes firewall, virtual private networks and encryption algorithms. Out of these, the virtual private network plays a vital role in preventing hackers from accessing the networks. Virtual Private Network (VPN) provides end users with a way to privately access information on their network over a public network infrastructure such as the internet.

There is a general saying in Nigeria that the youths are usually described as leaders of tomorrow. So many agree that the youths themselves are a reflection of the society. The nature of the socio-political and economic environment that prevails inside the country has imposed constraints in terms of meeting the needs and aspirations of the youths.

It could be very obtrusive that no country intending to greatness can afford to ignore the contributions of its children or permit them to constitute a major hazard to the realization of its regulations and programmes. Unfortunately, the modern social, financial

and political traits have left a bitter taste in the mouth of the kids; particularly, those from negative social and financial backgrounds. Apparently, the existing high fee for cash and other acquisitions regarded as yardsticks for determining the popularity of individuals within the society seems to have worsened the plight of the adolescents. This is because they have eroded the societal values for dignity of labour and moral integrity as they direct their energies closer to incomes a living via foul means.

It is thought provoking to imagine that some youths interact in cybercrimes at the expense of the country image. The Internet crimes are borne out of the truth that teenagers are not monitored through by their mother, father and schools. Some students are exposed through the Internet to unwholesome literature via studying junk mails. Some of them visit pornographic websites to share amusing with human beings of the other sex. It isn't fine for dad and mom and guardians to run permissive houses at the fee of their kids and wards [1]

While most cybercrimes are carried out to be able to generate earnings for cybercriminals, others are carried out against computer devices directly to harm or disable them, at the same time as others use computers or network to spread malware, illegal information, images or other materials. It is also confirmed that some cybercriminals do both, i.e. Target computer systems to contaminate them with viruses, which are then spread to different machines and every so often whole networks.

Notably, cybercrimes are of different classes in Nigeria; they range from Yahoo boys and their 419 Internet frauds; hacking; software piracy; pornography; credit score card or ATM fraud; denial of service attack; virus dissemination; phishing; cyber-plagiarism; cyber-stalking; cyber-defamation.

One can be questioning why the youth interact or involve in cybercrimes in Nigeria. Interestingly, cybercrimes like other criminal sports are especially motivated by certain situations considered one of that is urbanization. It is emphasized that urbanization without crimes is honestly impossible. The influx of the teenagers to cybercrimes is thriving amongst urban areas due to the fact the elite find it beneficial to put money into cybercrime as its miles a business that requires less capital.

The incidence of large scale of unemployment, harsh financial conditions and terrible educational systems also contribute immensely to the proliferation of cybercrimes in Nigeria. The youths are not facing the realities of canvassing vocational jobs where they discover it is very difficult to get a white collar job.

It is a component of worry consequently that the above notwithstanding that Nigeria isn't imposing stringent legislation to dissuade the young people from engaging in cybercrimes. Weak and fragile laws concerning cybercriminals exist in the country. The maximum unlucky is that the nation isn't adequately ready with sophisticated hardware to crack down the forensic criminals. Our regulation enforcement dealers are inadequately prepared in terms of personnel, intelligence and infrastructure to tackle the risk of cybercrimes that is adversely affecting the image and corporate identification of the country..

2. OVERVIEW OF CYBERCRIME

The term cybercrime has been major topic deliberated by so many with different views on the subject matter; a greater percentage coming at it from different angel than the others. Cybercrime have improved above conservative crimes and now have intimidating consequences to the national security of technologically developed countries.

Cyber attacks against financial services institutions are becoming more frequent, more sophisticated and more widespread. Although large-scale denial-of-services attacks against major financial institutions generate the most headlines, community and regional banks, credit unions, money transmitters, and third-party service providers (such as credit and payment processors) have experienced attempted breaches in recent years.

Following the documentation which affirms that “the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security”. The documentation went further to state that pressure could inaugurate from anywhere around the world, the problems are fundamentally international in range thus requires intercontinental cooperation, investigative support, and common substantive and procedural provisions”. In line with the above, Professor Augustine Odinma states that “cybercrime is any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, a phone, etc.

In every crime committed on the internet, the computer is either a target or used as a tool. For example, cyberstalking and hacking both involve attacking the computer, but the main target of a cyberstalker is the victim, not the computer. It is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system. When the individual is the

DOI: 10.31695/IJASRE.2019.33658

main target of the crime, the computer can be considered the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world. Human rather than mechanical weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the perpetrators all the more difficult. The essential concepts and motives have remained largely unchanged. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend [2][3][4]. Summarily, the following forms of internet crimes can be identified among others – software piracy, pornography, spamming (including cyberstalking, phishing, network intrusion, malware, viruses etc)

Crime as at this dispensation is perceived as a quiet perception, also a fundamental part of the peril we face as we go through life daily. In both intellectual and communal judgment, crime is concomitant with destruction and carnage. Moreover, we dearth unity on the most elementary point at issue "what is crime?" One theoretical designation is that crime, also called an injury or a criminal offence is an act harmful not only to some individual, but also to the hamlet or the state.

The cybercrime may be broadly classified into three groups. They are;

1. Crime against the Individuals: (a) Person (b) Property of an individual.

2. Crime against Organization: (a) Government (b) Firm, Company and Group of Individuals.

3. Crime against Society

The following are the crimes that have been committed against the followings group:

Against Individuals (a) Harassment via electronic mails (b) Dissemination of obscene material (c) Cyber-stalking (d) Defamation (e) Indecent exposure (f) Cheating (g) Unauthorized control/access over computer system (h) Email spoofing (i) Fraud.

Against Individual Property (a) Computer vandalism (b) Transmitting virus (c) Unauthorized access/control over computer system (d) Intellectual Property crimes (e) Internet thefts

Against Organization (a) Unauthorized access/control over computer system (b) Cyber-terrorism against the government organization (c) Possession of unauthorized information (d) Distribution of Pirate software.

Against Society (a) Child pornography (b) Indecent exposure of polluting the youth financial crimes (c) Sale of illegal articles (d) Trafficking (e) Forgery (f) Online gambling.

2.1. How Cyber Criminals Operate

Before the Internet, criminals had to dig through people's trash or intercept their mail to steal their personal information. Now that all of this information is available online, criminals also use the Internet to steal people's identities, hack into their accounts, trick them into revealing the information, or infect their devices with malware.

2.1.1. Who are Cybercriminals?

Most cybercrimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These "professional" criminals find new ways to commit old crimes, treating cyber crime like a business and forming global criminal communities.

Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities.

It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too, which can make things really complicated when a criminal launches an attack in another country.

2.1.2. Social Engineering

Social engineering is a tactic used by cyber criminals that uses lies and manipulation to trick people into revealing their personal information. Social engineering attacks frequently involve very convincing fake stories to lure victims into their trap. Common social engineering attacks include:

DOI: 10.31695/IJASRE.2019.33658

- Sending victims an email that claims there's a problem with their account and has a link to a fake website. Entering their account information into the site sends it straight to the cyber criminal (phishing)
- Trying to convince victims to open email attachments that contain malware by claiming it is something they might enjoy (like a game) or need (like anti-malware software)
- Pretending to be a network or account administrator and asking for the victim's password to perform maintenance.
- Claiming that the victim has won a prize but must give their credit card information in order to receive it.
- Asking for a victim's password for an Internet service and then using the same password to access other accounts and services since many people re-use the same password.
- Promising the victim they will receive millions of dollars, if they will help out the sender by giving them money or their bank account information.

2.1.3. Attack Techniques

Here are a few types of attacks cybercriminals use to commit crimes. You may recognize a few of them:

(a) Botnet - Are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

(b) DDoS Attacks - These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

(c) Cyber-stalking - This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

(d) Skimmers – This is the most common type of cybercrime in Nigeria where devices that steal credit card information when the card is swiped through them. This can happen in stores or restaurants when the card is out of the owner's view, and frequently the credit card information is then sold online through a criminal community.

This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government or banks benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails. Some identity thieves target organizations that store people's personal information, like schools or credit card companies. But most cyber criminals will target home computers rather than trying to break into a big institution's network because it's much easier.

(e) Cyber-terrorism - A cyber terrorist is a person who launches attack on government or organization with the aim of distorting and/or accessing stored information stored on the computer and their networks. The aim of a cyber terrorist is chiefly to intimidate a government or to advance his or her political or social objectives by launching various attacks against computers, network, and the information stored on them. It means that any act intended to instill fear by accessing and distorting any useful information in organizations or Government bodies using computer and internet is constitute cyber terrorism.

Cyber extortion is another form of cyber terrorism. In cyber extortion, a website, e-mail server, computer systems is placed under attacks by hackers for denial of services, demanding for ransom in return. Cyber extortionists mostly attack corporate websites and networks, cripple their ability to function and then demand ransom to restore their service.

(f) PUPs - PUPs or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install antivirus software to avoid the malicious download.

(g) Phishing or Man-In-The-Middle (MITM) - This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information, giving criminals access. How does this play out? Let's say you received an email that appeared to be from your bank, asking you to log in to your account to confirm your contact information. You click on a link in the email and are taken to what appears to be your bank's website, so you wouldn't hesitate to enter your login credentials after clicking the link in the email. But when you do that, you're not logging into your bank account, you're handing over your credentials to the cybercriminal.

(h) Prohibited/Illegal Content - This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating

DOI: 10.31695/IJASRE.2019.33658

terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

(i) *Online Scams* - These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

(j) *Exploit Kits* - Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

(k) *Drug Trafficking Deals* - Another form of cybercrime technique is Drug-Trafficking; it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at internet cafes, use courier websites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs.

(l) *Wiretapping/Illegal Interception of Telecommunication* - If telephone and network wiring lacks the necessary protection, wiretaps can pick up the data flowing across these wires. Criminals use wiretapping to eavesdrop on victim's communications. Sadly, it is rather easy to tap many types of network cabling. For instance, a simple induction loop coiled around a terminal wire can pick up most voices.

Telephone fraud has always been a problem among crackers, but with the increasing use of cellular phones, phone calling cards, and the ordering of merchandise over the phone using credit cards, this problem has increased dramatically in recent years in Nigeria. It's important to physically secure all networks cabling to protect it both from interception and from vandalism. It has been reported that the notorious.

.

3. CYBERCRIME IN THE NIGERIA (THE YAHOO-YAHOO BOYS/419 BOYS MENACE)

Cybercrime is one of the dominant forms of crime that is widely being perpetrated by youths in Nigeria. Indeed, the recognition of this growing acceptance of cybercrime, otherwise known as yahoo-yahoo in Nigeria, as a way of life among the youths has compelled the federal government to formulate measures to contain the trend at different points in time. The problem has, however, remained pervasive, despite past efforts put in place to curtail it.

Although cybercrime is not an exclusive preserve of Nigeria as it is a global phenomenon, yet the current unprecedented and massive involvement of Nigerians, especially the youths and mostly the university students in it, makes it a serious problem that requires urgent redress. According to [5], it is alarming that 80% of cybercrime perpetrators in Nigeria are students in various higher institutions. Indeed, many undergraduates in Nigerian universities have embraced internet fraud as a way of life; while many of them have become rich, some others have been caught by the law [6]. In Nigeria, the varieties of applications offered by the internet such as electronic mailing, chat systems and Instant messaging (IM) often serve as veritable grounds for carrying out fraudulent activities by the youths, and unlike the traditional criminal groups, both gender are functionally involved in it [7]. The antics of the 'yahoo yahoo boys', also known as 'yahoo yahoo millionaires' has raised a new generation of lazy youths, who spend hours on the internet perfecting their game and literally killing their prey [8]; cybercrime is becoming one of the fastest growing-internet (fraudulent) businesses in Nigeria [5]. Numerous crimes are committed on daily basis on the internet with Nigerians at the forefront of sending fraudulent and bogus financial proposals all over the world [9].

[7] observes that the technological advances have brought striking changes to Nigerian cultures, patterns of socialization, social institutions and social interactions. According to him, youths, especially undergraduates and the unemployed have embraced the information and communication inventions, such that the internet is accessed for most part of the day. [5] notes that cyber criminals in Nigeria are usually within the ages of 18 and 30 years, and are youths, who are outside the secondary schools, but are either in the university or are about to be admitted into the university. Similarly, a study conducted by the Youth against Cyber Crimes and Fraud in Nigeria (2018) shows that one out of every five youths in most cities in Nigeria is a cyber criminal. [10] & [7] claim that the anonymity and privacy that the internet provides for potential users has excessively enhanced the degree of fluidity and structural complexity of the 'yahoo-boys' operations in Nigeria. [11] similarly posit that the majority of cybercrimes perpetrated in Nigeria are mostly targeted at individuals and not necessarily computer systems, hence, they require less technical expertise. They further note that human weakness, such as greed and gullibility are generally exploited by cyber criminals; thus, damage done to their victim is usually financial and psychological.

[12] contend that cybercrime perpetrators in Nigeria have distinctive lifestyles from other youths and their strategies usually include collaboration with security agents and bank officials, local and international networking, and the use of voodoo (the

DOI: 10.31695/IJASRE.2019.33658

traditional supernatural power). [6] similarly observe that yahoo-boys in Nigeria enjoy a status of big boys; they are socially recognized among friends/lecturers/society and their flamboyant lifestyle entices others to desire to belong to the clique. The large scale involvement of Nigerians in cybercrime is a growing threat that has adversely affected the international image of Nigeria; the country is globally regarded as breeding ground of fraudsters and criminally minded people. Similarly, cybercrime continues to result in huge financial loss because cyber criminals often defraud their victims, large sums of money.

4. CYBER CRIMINALITY IN NIGERIA AS A SOCIETY

Crime tries to remains elusive and ever strives to hide itself in the face of development. Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence [13]. For Nigeria, in the battle against cybercrimes, efforts are now being directed at the sources and channels through which Cybercrimes are being perpetuated – the most popular one being Internet access points aided by insensitive ISPs.

Also cybercrimes have been in existence for only as long as the cyber space exists. This explains the unpreparedness of society and the world in general towards combating them. Numerous crimes of this nature are committed daily on the Internet with Nigerians at the forefront of sending fraudulent and bogus financial proposals all over the world. Nigeria has therefore carved a niche for herself as the source of what is now generally referred to as '419' mails named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud.

The contemptuous label of "cyber-criminals" is the figurative sword with which the Nigerian image is generally being hacked and left for dead. According to Professor Biko Agozino of Virginia Tech University, "there is a long standing demonization of Nigeria as being full of criminals." This unfortunate generalization, especially in the media, has a far-reaching negative impact on the overall image of Nigeria as a nation. It's become the prism with which most Nigerians are viewed and judged globally.

It stems from the country's vulnerability in a specific category of cybercrime known as '419' and its offshoots. Dr Mohamed Chawki, President of the International Association of Cybercrime Prevention, explains that the term 419 "is coined from section 419 of the Nigerian criminal code dealing with fraud. Nowadays, the axiom '419' generally refers to a complex list of offences which in ordinary parlance are related to stealing, cheating, falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts".

The most widely known component of '419' is cyber fraud - the culprit behind the blanket labelling of most Nigerians as cyber-criminals. But cybercrime in essence encompasses a wide range of crimes other than cyber fraud. These online crimes include cyberstalking, cyber hate speech, cyber espionage, cyber terrorism, cyber colonialism, revenge porn and cyber bullying among others. Nigeria is exclusively implicated in cyber fraud.

The key point here is that the term 'cybercrime' is misleading which is why it's reasonable to call into question Nigeria's reputation. It's an image nonetheless buttressed by the US Federal Bureau of Investigation (FBI) and its Internet Crime Complaint Centre which has ranked Nigeria third in the world behind the US and UK.

But the FBI centre's claims are problematic because in Nigeria cybercrime is exclusively cyber fraud (or scam). What constitutes 'cybercrime' in most Western nations differs from the particularities of cybercrime in Nigeria. They differ possibly because jurisdictional cultures and nuances apply online as they do offline.

Corruption among some government officers and some high profiled politicians also plays a role. Corrupt practices promote cyber criminal activities. Another contributory factor is the link between e-waste and online fraud. E-waste refers to discarded electronic appliances such as mobile phones and computers. The dumping of e-waste from countries such the UK and the USA is common in Nigeria and Ghana and there's a strong correlation between dumping and the physical locations of online fraud victims.

5. ROOT CAUSES OF CYBERCRIME AMONGST YOUTHS AND THE SOCIETY IN NIGERIA

With the huge and increasing population of Nigeria which presently stands at over 200 millions, we look at major causes of cybercrime among the youths and the society at large.

(a) Parents Influence/Negative Role Models

Youths are mirrors of the society, but it is quite unfortunate how parents neglect their rightful duties. Besides, it's miles saddening to look at that many parents transmit crime values to their wards, through socialization as if it is a social and cultural value which ought to be transmitted to the younger generation. The bad role version syndrome is having devastating effects on the lives of the youngsters related to in cybercrimes and other sharp practices.

DOI: 10.31695/IJASRE.2019.33658

[14] remarked that today many parents transmits crime values to their wards, via socialization as if it a socio cultural values which ought to be transmitted to the younger generation. Imagine a situation where the child supplies the father with vital information to wreck individual's banks account using the computer system, while the mother impersonates the account holder/owner at the bank. If this culture is imbibed among the younger generations most of them will see no wrong in cybercrime practices.

(b) Unemployment

Cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system. Most of the cybercrime happens today because Tertiary Institution Graduates fail to secure employments opportunities. According to the Nigerian National Bureau of Statistics, Nigeria is saddled with over 20 million unemployed people, with about 2 million new entrants into the dispirited realm of the unemployed each year. Youth Unemployment Rate in Nigeria averaged 23.63 percent from 2014 until 2018, reaching an all time high of 38 percent in the second quarter of 2018 and a record low of 11.70 percent in the fourth quarter of 2014. This clearly reveals that a lot of youths are not employed. There is an adage that says "an idle mind is the devils workshop"; as such most of our youth will use their time and knowledge as a platform for their criminal activity, in order to improve their livelihood and to make ends meet.

(c) Poor Remuneration from Law Enforcement Agencies

In the past years so many monies has been recovered from cyber activities and cybercriminals by the Law Enforcement Agencies namely the EFCC (Economic and Financial Crime Commission and the ICPC (Independence Corrupt Practices Commission) but most of the money recovered have not been injected into the economy or judiciously used for the benefits of the citizenry. It is also noticed that most of these agencies have cybercriminals on their payroll and as such make it very difficult to identify them and this in turn makes it impossible to arrest and convict them.

It is not enough to recover loots from cyber-criminals but accountability of these recovered loots matter most. This has been the challenge with Law Enforcement Agencies namely the EFCC (Economic and Financial Crime Commission) and the ICPC (Independence Corrupt Practices Commission). The looted proceeds are being re-looted by powerful officers and political figures thus demoralizing the efforts of those actually on the field yielding to the temptation of conniving with arrested cyber-criminals for an 'exchange' leading to their unlawful release. This has deprived the anti-graft agencies trust, dignity or integrity with the citizenry hence fettering the cause of cybercriminals who actually know they can buy their way out if by any chance they are apprehended.

Another challenge is the poor remuneration allotted the anti-graft agencies and their officers. These are officers recovering billions and trillions of Naira from cyber-criminals hence with massive opportunities to compromise their civil service allegiance and dignity.

(d) Weak Implementation of Cyber Crime Laws and Inadequate Equipped Law Agencies

The Nigerian legislation must implement strict laws regarding cybercriminals and when criminal offences occur, perpetrators must be punished for the crime they've committed because cybercrimes reduces the nation's competitive edge, failure to prosecute, cybercriminals, can take advantage of the weak gaps in the existing penal proceedings. Weak/fragile laws regarding cyber criminals exist in Nigeria, unlike in the real world were criminals such as armed robbers are treated with maximum penalties. Unfortunate the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012) state that "African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime" Nigeria is not an exception to this rule. Furthermore, it is therefore paramount that the nation's legislation should ensure proper implementation of their laws against cybercrime.

(e) Urbanization

Urbanization is one of the causes of Cybercrime in Nigeria; it is the massive movement of people from rural settlement to Cites. According to Wikipedia urbanization is looked at as the massive physical growth of urban areas as a result of rural migration in search for a better life. This result in a heavy competition amongst the growing populace more especially the elites, as such the elites find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest and they are popularly called "Yahoo Boys". [14]), in his article "Urbanization and cybercrime in Nigeria" reiterated urbanization as one of the major causes of cyber crime in Nigeria and Urbanization will be beneficial if and only if good jobs can be created in the cities where population growth is increasing, in his article, he emphasized that urbanization without crime is really impossible. As such the elites amongst them find it lucrative to invest in the cyber crime because it is a business that requires less capital.

(f) Police Collaborating with Fraudsters

The Nigerian Police Force and the SARS (Special Anti-Robbery Squad) operatives have played a very negative role within this period of the cybercrime boom. The situation where SARS men and women see the Yahoo Boys (Cyber Fraudsters) as an avenue of making quick cash even when they know these boys are cybercriminals. When these set of cybercriminals are caught by the police, it is so notable that the people who are expected to arrest them and bring them to

DOI: 10.31695/IJASRE.2019.33658

book are seen negotiating with the criminals to get percentage on the proceeds made from the illegal cyber activities and subsequently their unlawful releases.

(g) Quest for Quick Wealth

Another cause of cyber crime in Nigeria is quest for quick and unmerited wealth; there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Most cybercriminals require less investment and a conducive environment. Nigeria is a typical example of such an environment and many cybercriminals take advantage of that and scam people on their hard earned monies.

6. SOME BASIC TIPS TO GET PROTECTED FROM CYBERCRIME

Some easy tips to protect computers and mobile devices from the growing cyber threats:

Terminate Online Session Completely - Closing the browser window or typing in a new website address without logging out may give others a chance of gaining access to your account information. Always terminate your online session by clicking on the "Log out or Sign Out" button. Avoid using the option of "remember" your username and password information.

Create Backup of Important Data - Backup of all the important files whether personal or professional should be created. Getting used to back up your files regularly is the first step towards security of your personal computer.

Avoid Phishing emails: Be wary of potential phishing emails from attackers asking you to update your password or any other login credentials. Instead of clicking on the link provided in the email, manually type the website address into your browser.

Use Security Programs - If your system does not have data protection software to protect online, then by all means buy internet security program for your computer. Today, almost all new computer systems come with some kind of security programs installed.

Protect Your Password - Try creating a password that consists of a combination of letters (both upper case and lower case), numbers and special characters. Password should be changed regularly. Do not share your password with other people.

Participation in Social Networking - While participating in most social networking sites do not expose the personal information to others and all of these sites have a certain intensity of control over security issues. Use privacy settings to prevent personal information being broadcast.

Use a Two-Step-Authentication – If you are involved in any Instant messaging platform on your phone or computer, make sure you perform two-step-verification on all to avoid being a victim of cybercriminals. The verification allows you to know if anyone is trying to access your account or personal information from another device. The authentication platform sends you a code on your registered mobile device before any other transaction can be carried out.

Use Your Own Computer or Mobile Phone – It is generally safer to access your financial accounts from your own computer or mobile phone only. If you use some others computer or phone, always delete all the "Temporary Internet Files", and clear all your "History" after logging off your account.

Update Your Software Package Regularly - Frequent online updates are needed for all the Internet security software installed on your computer system. Be sure that your home Wi-Fi network is secure. Update all of the default usernames and passwords on your home router and all connected devices to strong, unique passwords.

Using Email - A simple rule in using this communication tool is not to open any links in emails from people you do not know. Hackers do use E-mail as the main target seeking to steal personal information, financial data, security codes and other. Do not use the link sent to you. If you need access to any website, visit the website by typing the address in your menu bar. Cybercrime, being a burning issue around the world, many countries is beginning to implement laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime. The laws in many countries on effectiveness of the punishment and prevention of computer crime requires a robust number and scope of the regulations, and even the proceedings, which lags far behind the reality of demand for computer crime in judicial practice.

7. POSSIBLE SOLUTIONS TO CYBERCRIME IN THE NIGERIAN SOCIETY

a. Cyber Ethics and Cyber Legislation Laws should be strictly adhered to:

DOI: 10.31695/IJASRE.2019.33658

Cyber ethics and cyber laws are also being formulated to stop cybercrimes in Nigeria and all over the world. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cybercrimes will reduce. African countries suffer various socio-economic problems such as food insecurity, social unrest, poverty, fuel crisis, AIDS, political and ethnic clashes and other conditions. This limits the strength of African nations to combat cybercrime effectively. However, it is necessary that Nigeria take measures to ensure that its penal and procedural law meets the challenges posed by cybercrimes. Government has to ensure laws are formulated and strictly adhered to.

b. Education:

Education is the most vital weapon for literacy, as such seminars and workshops should be organized from time to time with emphasis on cyber safety so that the individuals will learn to keep their personal information safe and youth will flee cybercrime. Cybercrime in Nigeria is difficult to prove as it lacks the traditional paper audit trail, which requires the knowledge of specialists in computer technology and internet protocols; hence We need to educate citizens that if they are going to use the internet, they need to continually maintain and update the security on their system. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

c. The Need for Individuals to Observe Simple Rules:

Internet users on their part ought to ensure proper anti-malware protection on their computer systems. There is the need for them to avoid pirated versions of software; and never to share their bank account personal details, Personal Identification Number (PIN), email access code (password) to unknown persons. Furthermore, internet users should never disclose any confidential information to anybody because none of these networks is foolproof or ultimately secure. Internet users should ignore any e-mail asking for any financial information. Also, there is need for the Telecommunications Regulatory Agencies in Nigeria (NCC – Nigerian Communications Commission) to enhance security on internet service providers' server to enable them detect and track cybercrimes.

d. Constant Training Programmes for Officials on Cybercrime:

For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight curb cybercrime, it is recommended that there is need for them to understand both the technology and the individuals who engaged in this criminal act. These government personnel working to ensure these cybercriminals are arrested and given justice to their atrocious deeds should be given regular advanced technological trainings and seminars in cybercrime and ICT from other developed countries that has better knowledge in fighting this menace.

e. Provision of Jobs by Government:

Government should create job opportunities for the growing number of unemployed youths who see cybercrime as the only means of survival and making quick wealth just as they see the government official's loot so much from tax payers' money. This will help to minimize the menace. Empowerment programmes should also be a regular exercise to keep the youths busy; an example of this type of empowerment is the N-Power programme which enables the youths to access skills acquisition and development. Most of these kinds of initiatives by the government can also be injected into the society to better the lives of the youths.

8. CONCLUSION AND RECOMMENDATIONS

Nigeria has lost so much reputation and bilateral trade options from foreign nations. The businesses and investment which was suppose to get into the country goes away because of the huge presence of cybercrime and cybercriminals who debuts and pretend as government officials, lure these foreign investors and dump them subsequently.

Taking measures to secure your own computer and protect your personal information, you are not only preventing cybercriminals from stealing your identity, but also protecting others by preventing your computer from becoming part of a botnet.

It is glaring and obvious that cybercrimes cannot be easily eliminated, but it can certainly be minimized. With the collaborative efforts of all stakeholders like individuals, corporate organizations and government to nip the scourge in the bud. Government in any respect levels ought to also ensure that its legal guidelines practice at cybercrimes. It is vital that Nigeria as a nation takes measures to make sure that its penal and procedural laws are adequate to fulfill the challenges posed with the aid of cybercrimes. Not most effective this, government should make sure that regulations are formulated and strictly adhered to regardless of the

DOI: 10.31695/IJASRE.2019.33658

repute and character of the humans involved. We believe that creation of job possibilities for the teeming unemployed youths will limit the threat drastically.

A combination of sound technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cyber criminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cybercriminals. Government should also make provision for intensive training of law enforcement agencies on ICT so that they can track down the cybercriminals no matter how intelligent and cunning they may be.

In our rapidly evolving connected world, it is very important to understand the types of threats that could compromise the online security of your personal information. Stay informed and make sure your devices are fortified with proper security measures.

REFERENCES

1. Ajibike T. (2019) "Youth and Cybercrime in Nigeria", Punch Newspaper, March 15.
2. Cooper, A., McLaughlin, I.P., & Campbell, K.M. (2000). Sexuality in cyberspace: update for the 21st century. Cyber Psychology & Behavior Vol. 34, pp.521–536.
3. CP80 (2005): Port Channeling Technology: The Next Evolutionary Stage of the Internet. Available Online at www.cp80.org.
4. CP80 (2007): Empowering Families on the Internet. Available online at http://www.intgovforum.org/May_contributions/CP80 20Foundation contribution.pdf
5. Aghatise, E. J. (2006). Cybercrime definition. Computer Research Centre, Retrieved from http://www.crime-research.org/articles/joseph06/2.
6. Tade, O., & Aliyu, A. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2), pp.860-875.
7. Adeniran, A. I. (2008). The Internet and Emergence of Yahoo-boys Sub-culture in Nigeria. International Journal of Cyber Criminology, 2(2), pp.368-381.
8. Nkanga, E. (2008). Combating Cyber Crime Menace in Nigeria. Retrieved on 15th January 2012 from ThisDay.www.allafrica.com
9. Longe, O, Omoruyi, I & Longe, F (2005): Implications of the Nigeria Copyright Law for Software Protection. The Nigerian Academic Forum Multidisciplinary Journal. Vol. 5, No. 1. pp7-10.
10. Reddick, R., & King, E. (2000). The Online Student: Making the Grade on the Internet. Forth Worth: Harcourt Brace.
11. Longe, O. B., & Chiemeke, S.C. (2008). Cyber crime and Criminality in Nigeria - What Roles are Internet Access Points Playing? European Journal of Social Sciences, 6(4), pp.132-139.
12. Aransiola, J., & Asindemade, S. (2011). Understanding Cyber Crime Perpetrators and the Strategies they employ in Nigeria. Cyberpsychology, Behavior, and Social Networking, 14(12), pp.759-63.
13. Sylvester, Linn (2001): The Importance of Victimology in Criminal Profiling. Available online at: http://isuisse.ifrance.com/emmaf/base/impvic.html
14. Meke S.E. N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".

DOI: 10.31695/IJASRE.2019.33658