Villanova Journal of Science, Technology and Management

Vol. 2. No. 1. 2020. ISSN: 2672-4995 (Online) 2672-4987 (Print)

CHALLENGES AND WAY OUT OF CYBER SECURITY ISSUES IN NIGERIA

Adenusi Dauda A.[a]*, Adekunle A. U.[b], Ekuewa J.B.[c], Ayediran O.R.[d],
[aa]Ibadan City Polytechnic, P.M.B. 10426, Ibadan, Oyo State.
[bb]Federal Polytechnic Ede, P.M.B.231, Ede, Osun State.
E-mail: daudaadenusi2006@yahoo.com Tel: 08163302988/08063634490

Abstract

Cyber-space is a platform where you can process, receive and send information. It includes phone set, computer system, network, information stored on the network, network devices, all this constitute what is being called Cyber space. This cyber space is not secure, and the process to make it secure is known as Cyber Security. **.** *Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. The Internet is one of the fastest-growing areas of technical infrastructure development. Google, Wikipedia and Bing to mention a few, give detailed answers to millions of questions every day. Cyberspace is a world that contains just about anything one is searching for. With the advent of these advancements in information accessibility and the advantages and applications of the internet comes an exponentially growing disadvantage- Cyber Crime. Cyber security has risen to become a national concern as threats concerning it now need to be taken more seriously. This paper attempts to provide an overview of Cybercrime and Cyber-security. It defines the concept of cybercrime, identify reasons for cyber-crime and its eradication. It looks at those involved and the reasons for their involvement. Methods of stepping up cyber security and the recommendations that would help in checking the increasing rate of cyber-crimes were highlighted. The paper also attempts to name some bottleneck of cybercrime and present practical and logical solutions to these threats.*

Keywords: Cyber-space, Cyber-security, Cyber-crime, ICT, Internet

INTRODUCTION

From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts.[13] This paper hopes to paint a developing scenario of the evolution of new type of war - the internet cybercrime - which will cause destruction of greater magnitude than the two past world wars- if not properly nipped in the bud. It has been established that Nigeria is an impressionable country. The advent of the internet to her was both welcome and full of disadvantages. The exceptional outbreak of cyber-crime in Nigeria in recent times was quite alarming, and the negative impact on the socio-economy of the country is highly disturbing.

Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear from the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users. The first recorded cyber murder was committed in the United States some years ago, according to the Indian Express, January 2012, an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient.[10] Statistically, all over the world, there has been a form of cyber-crime committed every day since 2016.[15] Prior to the year 2001, the phenomenon of cyber-crime was not globally associated with Nigeria. This resonates with the fact that in Nigeria we came into realization of the full potential of the internet right about that time. Since then, however, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the internet.[14] Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals are no longer suitable to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters.[18] Since the issue of cyber security is raising a number of questions in the minds of Nigerians, it is only fair that we answer these questions. This paper seeks to give an overview of cyber-crime and cyber-security, its challenges and proffer solutions.

LITERATURE REVIEW

The issue of cyber-crime is one that has been discussed by many people with various perspectives on the issue, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries such as the United States.[7] According to a publication [20] which states 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 publication further stated that since threats could originate anywhere around the globe, the challenges are inherently international in scope thus requires international cooperation, investigative assistance, and common substantive and procedural provisions". In line with the above, Professor Augustine Odinma states that "cyber-crime 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 computers and phones etc. The illegal act may be targeted at a computer network or devices e.g., computer virus, denial of service attacks

(DOS), malware (malicious code). The illegal act may be facilitated by computer network or devices with target independent of the computer network or device".[5] Relating cyber-crime to the military in a paper depicting his vested interest in the country's military well-being, Major General Umo outlines that cybercrime, cyber terrorism, cyber warfare, cyber security are one and the same thing. This is because, stealing or forgery directed at an individual or an organization is synonymous to waging war on the target of the crime.[4]

Statistically, Nigeria ranked 43 in EMEA and ranked third among ten nations that commits cyber-crime in the world.[5] Professor Oliver Osuagwu, relating cyber-crime to the collapse of the educational sector, points out that cybercrime is causing near total collapse of the education community, particularly in Nigeria, with over 90% of criminals coming from this sector. Wrong value system has been identified as key factor encouraging cybercrime in Nigeria and the desire to get rich quick without working for it. Cyber-crime is complex and committed mostly from remote locations making it difficult to police. The absence of enabling law makes policing even more difficult.[9] As earlier stated, the internet has a capacity for more good than bad. This is better explained by Mrs. R. Moses-Oke [14] when she said "The oxymoronic nature of the Internet is one of its unforeseen attributes; at its inception, no one, perhaps, could have clearly foreseen that, and how, the Internet would someday become a veritable platform for globalized criminal activities. As has been copiously remarked, the benefits of the Internet have so often been tainted by its versatility for virtual criminal activities that have vastly devastating physical and social impacts". Many will agree that concerns are increasing as Nigeria is increasing its digitalization not only in the area of commerce and communications, but gradually into the area of electronic banking. In the past years, electronic banking and the cashless initiative have been in focus a lot. Amaka Eze in her article [12] for THISDAY live writes, "As the country integrates electronic payment system into its financial institution; a step that is expected to accelerate the nation's e-commerce growth, the negative impact of cybercrime on businesses, and the absence of appropriate laws to guarantee the legality of online transactions, continue to create fear in the mind of users and potential online users". Even as we talk about the rise and dangers of cyber-crime and breach in cyber security, there is need to focus on a way to reduce or completely eradicate its incidence in Nigeria. To restore the full glory of cyber security, those involved have to spend time to learn how cybercrime ring operates and then devise strategies to fight the menace. We cannot fight today's crime with yesterday's technology. It will always be a losing battle if security professionals are way behind the cyber criminals in terms of technological knowledge. It's not just about computing skills, but IT Security expertise.

Also discussed previously are the costs incurred by the government due to the rise of cyber-crime. As for measuring costs, the Detica report in [3] considered four categories: costs in anticipation of cybercrime, such as antivirus software, insurance and compliance; costs as a consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise; costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies; indirect costs such as reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy. Having seen cybercrime from different perspectives, we would now discuss fully on cyber-crime and cyber-security, practical instances and solution mechanisms in the following sections. Much has already been done by the law enforcement agents, but cyber-crime is still perpetrated underground.

OVERVIEW OF CYBER-CRIME AND CYBER-SECURITY

As technology has developed so also the definitions of cyberspace, cyber security and cybercrimes. It has been argued that since computer crime may involve all categories of crime, a definition must emphasize the particularity, the knowledge or the use of computer technology.

Cyber-space is a platform where you can process, receive and send information. It includes computer system, our network, information stored on the network, network devices that you can connect to the network, all these constitute what we call Cyber space. Including your phone set. They are all cyber space. This cyber space is not saved, and the process to make it save is what we called Cyber Security**.** Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.[20] Cyber-security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks. Cyber-crime refers to the series of organized crime attacking both cyber space and cyber security. Sophisticated cyber criminals and nation-states, among others, present risks to our economy and national security. Nigeria's economic vitality and national security depend on a vast array of interdependent and critical networks, systems, services, and resources known as cyberspace. Cyber-space has transformed the ways we communicate, travel, power our homes, run our economy, and obtains government services.

Cyber-security is the body of technology, processes and practices designed to protect networks, computers, programs and data from attacks, damage, or authorized access. In the computing or cyber context, the word security simply implies Cyber-security.[19]

Ensuring cyber-security requires coordinated efforts from both the citizens of the country and the country's information system. The threat posed by breaches in our cyber-security is advancing faster than we can keep up with. It is not possible to concentrate efforts on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. This leads us to conclude that we have to attack cyber security breaches as a whole. What then are these breaches?

Cybercrime includes unlawful actions carried out on or by means of a computer such as internet fraud or use of computer to commit numerous crimes such as email scams – to cheat unsuspecting people, hacking – by people who create viruses intentionally to gain access and harm computer data.

Others are introducing worms to destroy computer data, stealing data, stealing people identity, obtaining money under false pretense (i.e 419) and introducing malicious traffic from many source to make real services unavailable to a company server etc.

Cybercrimes take advantage of speed on the internet, messaging system and publications of information globally in seconds, to attack computer systems with their cruel plans.

Cyber-crime refers to criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the internet to steal personal information from other users.[6] Perhaps the most complete definition of Cyber-crime is as given: [7]

> "A criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), system interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud".

GOALS OF CYBER SECURITY

The following are the objectives of Cyber-security.

1. To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
2. To help individuals and institutions develop and nurture a culture of cyber security.
3. To work collaboratively with public, private and international entities to secure cyberspace.

4. To help understand the current trends in IT/cybercrime, and develop effective solutions.
5. Availability.
6. Integrity, which may include authenticity and non-repudiation.
7. Confidentiality.

E-CRIMES THAT ARE PECULIAR TO NIGERIA

There is no doubt that e-crime is an image trauma for Nigeria. Cyber-crime is a source of concern and embarrassment for the nation. The internet creates unlimited opportunities for commercial, social, and educational activities. But as we can see with cyber-crime the internet also introduces its own peculiar risks. The instances reported here ranges from fake lotteries to the biggest internet scams. Elekwe, a chubby-faced 28-year-old man made a fortune through the scam after two years of joblessness despite having Diploma in Computer Science. He was lured to Lagos from Umuahia by the chief of a fraud gang in a business center. He has three sleek cars and two houses from his exploits. In July 2001, four Nigerians suspected to be operating a "419" scam on the internet to dupe unsuspecting foreign investors in Ghana were arrested by security agencies. Their activities are believed to have led to the loss of several millions of foreign currencies by prospective investors. Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under false claims. They were arrested at the point of delivery by government officials. Mike Amadi was sentenced to 16 years imprisonment for setting up a website that offered juicy but phony procurement contracts. The man impersonated the EFCC Chairman, but he was caught by an undercover agent posing as an Italian businessman. The biggest international scam of all was committed by Amaka Anajemba who was sentenced to 2½ years in prison. She was equally ordered to return $25.5 million of the $242 million she helped to steal from a Brazilian bank.

An internet scam case was reported on the Sunday PUNCH newspaper of Sunday, July 16, 2006 involving a 24-year-old Yekini Labaika of Osun State origin in Nigeria and a 42-year-old nurse of American origin, by name Thumbelina Hinshaw, in search of a Muslim lover to marry. The young man deceived the victim by claiming to be an American Muslim by the name, Phillip Williams, working with an oil company in Nigeria and he promised to marry her. He devised dubious means to swindle $16,200 and lots of valuable materials from the victim. The scammer later was sentenced to a total of 19½ years having been found guilty of eight-counts against him. Incidences like these are on the increase. Several young men unabated are still carrying out these illegal acts successfully, ripping off credulous individuals and organizations.[8] Recently, a report indicated that Nigeria is losing about $80 million yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa.

The American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up to 90% in 2015. The Centre also ranked Nigerian cyber-crime impact per capital as being exceptionally high.[17]. Those involved are between 18-25 years mostly resident in the urban centers. The internet has help in modernizing fraudulent practices among the youths. Online fraud is seen as the popularly accepted means of economic sustenance by the youths involved. The corruption of the political leadership has enhanced the growth of internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud.[1]

Recent convicted Nigerians that are into cybercrime are:

1. Olayinka Olaniyi, 34, of Nigeria was sentenced to five years, 11 months in prison, to be followed by three years of supervised release on October 22, 2018. Olaniyi was also ordered to pay restitution in the amount of $56,175.44.
2. Damilola Solomon Ibiwoye, 29, of Nigeria was sentenced to three years, three months in prison to be followed by three years of supervised release on January 31, 2018. He was also ordered to pay $56,175.44 in restitution.
3. Bonaventure Sunday Chukwuka, 41 of Roding Gardens, Loughton, who was found guilty of conspiracy to commit fraud by false representation, and conspiracy to conceal/transfer criminal property (money laundering). He was also found guilty of possession of a prohibited item (a phone) in prison. Chukwuka was sentenced to 11 years' imprisonment.
4. Andrew Chike Chukwu, 35 of River Road, Buckhurst Hill, who was found guilty of conspiracy to commit fraud by false representation and conspiracy to conceal/transfer criminal property. He was handed 10 years' imprisonment.
5. Emmanuel Chike Chukwuka , 27 of Roding Gardens, Loughton, was found guilty of conspiracy to commit fraud. He was found not guilty of conspiracy to money launder and was sentenced to two years and eight months' imprisonment.
6. Christian Chukwuka, 39 of Latchetts Shaw, Basildon, Essex was found guilty of conspiracy to commit fraud by false representation and conspiracy to conceal/transfer criminal property. He got five years and nine months' imprisonment.
7. Queen Chukwuka, 32 of Roding Gardens, Loughton was found guilty of acquiring/possessing criminal property and was sentenced to a community order.
8. Grace Plange Chukwu, 39 of River Road, Buckhurst Hill, was found guilty of acquiring/possessing criminal property. She, however, got a conditional discharge.

The court heard during the trial that Bonaventure Chukwuka led an organised criminal gang that targeted businesses and individuals by hacking into their email accounts, and stealing large sums of money. This case was investigated by the Federal Bureau of Investigation.

CATEGORIES OF CYBER CRIME

a. **Identity Theft:** Identity theft occurs when a hacker steals information from personal accounts such as banking information, social security numbers, and addresses. The hacker will then use this information to create accounts in the victim's name. Being aware of encrypted websites and having adequate measures of protection when imputing this information into websites is essential to even the less-than average user of internet.

b. **Viruses:** Computer viruses are pieces of code that are usually attached to downloadable files. When the file is running, the code of the virus activates and proceeds to spread throughout computer files. These viruses infect vital information and can lead to deletion or corruption of important system files. Some viruses will also allow personal information and files to be accessed by another user.[16]

c. **Cyber Stalking:** Cyber stalking is a crime that occurs when a person is being harassed by another person in an online setting. The victim is often bombarded with messages not just to themselves, but also to family members or friends. Threats are often received by the victim as a tactic to get the victim to reply. Often the victim will suffer from anxiety and fear.

d. **Phishing:** A "phishing scam" is the act of sending fraudulent emails that appear to come from legitimate enterprises for the purpose of tricking the victim into providing personal information, including usernames and passwords. It is important for a potential victim to be aware of email addresses associated with bank accounts and other sites that may contain personal information. Olaniyi and Ibiwoye directed phishing emails to college and university employees. Once they had possession of employee's logins and passwords, they were able to steal payroll deposits by changing the bank account into which the payroll was deposited. [17].

e. **Hacking:** Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what you do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

f. **Spamming**– involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.

g. **Cyber laundering**- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

h. **Website Cloning:** One recent trend in cyber-crime is the emergence of fake 'copy-cat' web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

EMERGING CYBER TRICKS IN NIGERIA

a. **Beneficiary of a Will Scam**: The criminal sends e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.

b. **Online Charity**: Another aspect of e-crime common in Nigeria is where fraudulent people host websites of charity organizations soliciting monetary and materials donations to these organizations that do not exist. Unfortunately, many unsuspecting people have been exploited through this means.

c. **Next of Kin Scam**: Collection of money from various bank and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative.

d. **The "Winning Ticket in Lottery you Never Entered" Scam:** These scams lately include the State Department's green card lottery. This allows users to believe they are beneficiaries of an online lottery that is in fact a scam.[18]

e. **Bogus Cashier's Check**: The victim advertises an item for sale on the internet, and is contacted

f. **Computer/Internet Service Time Theft**: Whiz kids in Nigeria have developed means of connecting Cyber Cafes to Network of some ISPs in a way that will not be detected by the ISPs and thereby allow the Cafes to operate at no cost.

CHALLENGES OF CYBERCRIME

a. **Domestic and International Law Enforcement**: A hostile party using an internet connected computer thousands of miles away can attack internet- connected computers in Nigeria as easily as if he were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.

b. **Unemployment**: The spate of unemployment in Nigeria is alarming and growing by the day. Companies are folding up and financial institutions are going bankrupt.

The federal government has proposed a mass sack of government workers. Companies are also embarking on mass sacks of staff. Financial institutions have put unreasonable age barriers on who is eligible to apply for jobs and embark on mass lay-offs of staff based on ad-hoc decisions.

c. **Poverty Rate**: On the global scale, Nigeria is regarded as a third world country. The poverty rate is ever increasing. The rich are getting richer and the poor are getting poorer. Insufficient basic amenities and an epileptic power supply have grounded small scale industries.

d. **Corruption**: Nigeria was ranked third among the most corrupt countries in the world. Until 1999, corruption was seen as a way of life in Nigeria.

e. **Lack of Standards and National Central Control**: Charles Emeruwa, a consultant to Nigeria Cyber Crime Working Group (NCCWG), said lack of regulations, standards and computer security and protection act are hampering true e-business. Foreign Direct Investment (FDI) and foreign outsourcing are encouraging computer misuse and abuse.

f. **Lack of Infrastructure**: Proper monitoring and arrest calls for sophisticated state of the art Information and Communication Technology devices.

g. **Lack of National Functional Databases**: National database could serve as a means of tracking down the perpetrators of these heinous acts by checking into past individual records and tracing their movements.

h. **Proliferation of Cybercafés**: As a means of making ends meet, many entrepreneurs have taken to establishment of cybercafés that serve as blissful havens for the syndicates to practice their acts through night browsing service they provide to prospective customers without being guided or monitored.

i. **Porous Nature of the Internet**: The Internet is free for all with no central control. Hence, the state of anarchy presently experienced.

REASONS FOR ATTACKING PEOPLE, ORGANIZATION AND GOVERNMENT

As you think of how to prevent cybercrime and internet fraud in Nigeria, you would also wonder why cyber criminals attack people in the internet, organization and governments all over the world.

Here are some reasons

1. The prime reason is greed for money by these criminals
2. Unemployment is partly to blame for this crime. Undergraduate leave Nigeria institutions of Higher Learning yearly without any hope of employment.
3. Lack of confidence in your ability to succeed in a legitimate way.
4. Bad upbringing caused by the absence parents contributes to nurturing criminals
5. Peer pressure could lead young innocent ones into this crime
6. Attraction for fast money by youths is a factor of cybercrime
7. Porous cyber security protocol by organization, government and individuals

8. Disregard for the rule of law because it fails to punish these criminals to deter others.
9. Lack of accountability of government officials is another cause of this crime.

WHO ARE THE TARGETS OF THESE CRIMINALS?

To find how to prevent cybercrime and internet fraud in Nigeria, let us find out the targets of these criminals.

Everyone who uses a computer is a target but the most affected is the financial sector. Nigerian banks are going cashless and using more electronic means of payment which leads to the generation of massive data. From 2014 to 2018, Nigerian banks have lost over N198 billion by electronic fraud and cybercrime. In addition, Cyber criminals target and wreak havoc to computer systems of all facilities and government establishments.

This quotation by the National Security Adviser to President Mohammadu Buhari says, "Nigeria loses N127 billion annually to cybercrime". That is how devastating the effect of cybercrime is to Nigeria. Hence, fighting and defeating it is the only way forward.

Moreover, it is embarrassing when foreign countries catch Nigerians who commit cybercrimes. Till date, Nigeria suffers from the stigma of 419 put on the nation in the 90's. according to the President of integrated Cyber Security Solution, in 2015 Nigeria lost an estimate of N40 billion naira to cyber criminals and globally the world lost the sum of $400 billion. We should not allow this huge waste of our scarce resources to cybercrime to continue if we don't want it to cripple the economy and turn citizens into paupers.

EFFECTS OF CYBER CRIME

a. Financial loss: Cybercriminals are like terrorists or mental thieves in that their activities impose disproportionate costs on society and individuals [11].
b. Loss of reputation: Most companies that have been defrauded or reported to have been faced with cybercriminal activities complain of clients losing faith in them.
c. Reduced productivity: This is due to awareness and more concentration being focused on preventing cybercrime and not productivity.
d. Vulnerability of Information and Communication Technology (ICT) systems and networks.

WAYS TO PREVENT CYBERCRIME IN NIGERIA.

How to prevent cybercrime in Nigeria like any other crime is difficult as criminals use available sophisticated technology and international criminal networks to improve their skill for carrying out their tricky plans.

The following are ways to fight Cybercrime and internet fraud:

1. **Increasing Security of Computer and Networks**

Increasing security of computer and networks by developing software and methods to counter potent software hacker tools such as automatic computer virus generators. Internet listening sniffers, password guessers, vulnerability testers and the dreaded computer service saturators.

2. **Simple and Advanced Methods for Preventing Cyber Crime**
   You can prevent computer crimes by protecting computer screens from inspection, locking printed information and computers in safe places, backing up software and data files to keep copies safe and removing sensitive material and information from your table during and after work hours.
   In addition, using these more advanced ways of how to prevent cybercrime and internet fraud in Nigeria is effective. They include adopting encryption procedures, giving software usage permissions to authorized users, requesting passwords to use a computer, fixing firewalls and systems that detect unauthorized entrance and finally using self-regulating controls in a computer system.
3. **ICT Ability of Personnel**
   Security personnel must have Information Communication Technology (ICT) capability, training and adequate knowledge of computer (software and hardware) to win this war.
4. **First Class Intelligence Capability of the Security Forces**
   To commit cybercrime and succeed, you must know how to manipulate information by using advanced technology and software. The criminals seem to be ahead of the security forces and have more sophisticated equipment too. Security forces intelligence gathering ability must be a head of the bad guys. If you want to fight the menace to a standstill.
5. **Adequate Plan**
   The Nigeria Security personnel should spend enough time to profile these attacks and plan to prevent them and if possible, catch these criminals in the act.
6. **Support by Main One**
   As you seek for how to prevent cybercrime and internet fraud in Nigeria using Main One is a brilliant idea [7]. What is main one? Main One is the first connectivity and data provider in the country. It could use its cyber security solutions to help its customers such as telecommunication providers. Banks, oil and energy companies direct traffic through Main One's distributed Denial of Service (DDOS) protection system to check cybercrime before it happens.

7. **Develop Local Solutions by Technology Transfer**
   Government's use of Technology transfer project to develop local solutions by partnering with Leo Telecommunications Limited an Israeli company, to set up a security and Defense technology. Assembly plant for Security and communications hardware and software solutions will prevent cybercrime and internet attacks.
8. **Government Support for the Niger Cyber Crime Working Group**

Government should support The Nigeria Cyber Crime Working group set up by former President, Olusegun Obasanjo to stop cybercrime in Nigeria. Funding this group and giving them good equipment will help them provide new ways of preventing this crime.

9. **Removing Unsecure Wireless Connections**
   The Government should borrow a leaf from the United States and remove all unsecure Wireless connections in the country as they did in America.
10. **Development of Local ICT Solutions**
    National Computer Society should build a platform to develop local methods of using Information Communication Technology to secure the country against cyber bandits.
11. **Declare Computer Emergency**
    The government has set up Computer Emergency response teams in National Security Adviser's office and National Information Development Agency. These teams should work with start-up companies going into technology business to build secure computer Networks for government and stop cybercrime and internet fraud in Nigeria.
12. **Free Education and Vocational Training**
    Government should give Youth free education and vocational training to give them more opportunities to have decent jobs and live comfortable lives.

CONCLUSION

In conclusion, how to prevent cybercrime in Nigeria is tough but doable. Using simple and advanced methods such as protecting computer screens from inspection, encryption, firewalls and passwords to make computer databases strong is the way to go.

In addition, training law enforcement staff in ICT and use of first rate equipment will help nip these crimes in the bud and having fast trials to get judgment quickly against these criminals will deter others.

Finally, all citizens must be alert to the danger of cybercrime and support government as they try to rid society of these criminals, save billions of naira and inject the same to build needed infrastructure and grow the economy.

REFERENCES

[1] Adebusuyi, A. (2008): *The Internet and Emergence of Yahooboys sub-Culture in Nigeria*, International Journal Of Cyber-Criminology, 0794-2891, Vol.2(2) 368-381, July-December

[2] Amaka Eze, "Thisday Live"

[3] Anderson, Ross, et al. (2016): *Measuring the cost of cybercrime*, 11th Workshop on the Economics of Information Security (June 2016), Retrieved from http://weis2016.econinfosec.org/papers/Anderson_WEIS2012.pdf

[4] Augustine C. Odinma, MIEEE (2010): *Cybercrime & Cert: Issues & Probable Policies for Nigeria*, DBI Presentation, Nov 1-2.

[5] Background Check International, *"Information Technology/Cyber Security Solutions"*

Ibikunle. F. and Eweniyi O. (2017): Cyber Security In Nigeria. *(IJCRSEE) International Journal of Cognitive Research in science, engineering and education. Vol. 1, No.1, 2017.*

[6] International Telecommunication Union, Retrieved from http://www.itu.int/en/Pages/default.aspx

[7] Laura, A. (2015): *Cyber Crime and National Security: The Role of the Penal and Procedural Law"*,Research Fellow, Nigerian Institute of Advanced Legal Studies., Retrieved from http://nials-nigeria.org/pub/lauraani.pdf

[8] Longe, O. B, Chiemeke, S. (2018): *Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access Points In Playing?, European Journal Of Social Sciences – Volume 6, Number 4*

[9] Major General G. G UMO (2010): *Cyber Threats: Implications For Nigeria's National Interest,* Retrieved from https://docs.google.com/file/d/0B9sby6N_v5O3M2FlNWIzZjgtMDRiOS00NjI1LThmMjItNmI0Nzg5NGVlNTM2/edit?num=50&sort=name&layout=list&pli=1

[10] Mohsin, A. (2006): *Cyber Crimes And Solutions*, Retrieved from http://ezinearticles.com/?Cyber-Crimes-And-Solutions&id=204167

[11] Okonigene, R. E., Adekanle, B. (2009): *Cybercrime In Nigeria,* Business Intelligence Journal, Retrieved from http://www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7.pdf

[12] Oliver, E. O. (2010): *Being Lecture Delivered at DBI/George Mason University Conferenceon Cyber Security holding,* Department of Information Management Technology Federal University of Technology, Owerri, 1-2 Nov.

[13] Olumide, O. O.,Victor, F. B. (2010): *E-Crime in Nigeria: Trends, Tricks, and Treatment*. The Pacific Journal of Science and Technology, Volume 11. Number 1. May 2010 (Spring)

[14] Roseline, O. Moses-Òkè (2012): *Cyber Capacity Without Cyber Security: A Case Study OfNigeria's National Policy For Information Technology (NPFIT),* The Journal

Of Philosophy, Science & Law Volume 12, May 30, 2012, Retrieved from www.Miami.Edu/Ethics/Jpsl

[15] Schaeffer, B. S., et al. (2018): *Cyber Crime And Cyber Security: A White Paper For Franchisors, Licensors, and Others*

[16] Strassmann, P. A. (2014): *Cyber Security for the Department Of Defense*, Retrieved July 10, 2017 From http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf

[17] Department of Justice, U.S. Attorney's Office, Northern District of Georgia (2018) "Cyber-criminal sentenced for hacking universities"

[18] Thompson, D. (1989): *Police Powers-Where's the Evidence*, *Proceedings of the The Australian Computer Abuse Inaugural Conference*.