

CYBER CRIME AND STRATEGIES FOR REDUCING ITS MENACE AMONG NIGERIAN YOUTH THROUGH PROPER IMPLEMENTATION OF CYBER SECURITY AND EMPLOYMENT CREATION

MAXIMUS CHIJOKE

Chukwuemeka Odumegwu Ojukwu University
Igbariam Campus, Anambra State

&

CLARA ONYINYE AJIBO

Chukwuemeka Odumegwu Ojukwu University
Igbariam Campus, Anambra State

&

ANTHONY CHUKWUMA ERUKA

Ximusobt2000@yahoo.com

+2348083703900

Chukwuemeka Odumegwu Ojukwu University
Igbariam Campus, Anambra State

Abstract

Crime is as old as man. So far that society exists, there must be good and evil. Evil permits the existence of crime. However, this paper examined cyber crime and strategies for reducing its menace among Nigerian youth through proper implementation of cyber security and employment creation. It strongly recommends that the religious bodies should preach against the evil of cyber crime that is destabilizing the youth and societal growth and development. Again, it recommends that the government should provide employment opportunities for the youth thereby giving them the space for personal growth and to contribute to the development of the society at large.

Keywords: crime, cyber crime, cyber security, youths, employment creation.

Introduction

Crimes have been seen as issues of concern in the world at large since the fall of Adam and Eve. Crime and criminality have been identified as challenges to the development of many countries of the world with peculiar reference to Nigeria. Nigeria as a country has fought the cyber crime through proper implementation of cyber security and employment generation. These efforts, notwithstanding, many lose their money and valuables on daily basis to the high rate of cybercrime and other forms of fraud which are attributed to unemployment. It is therefore necessary for all and sundry to properly checkmate youth on the wrong use of internet. Cybercrime is retrogressive to national development in many ways. Crime is seen as gravely injurious to development; it brings about economic and social downfall of any given society.

The concept of cyber crime

Cyber crime is seen as criminal activity that targets uses a computer, a computer network or networked device to deceive individual of different kinds. This is committed by cybercriminal or hackers who want to make cash online by crooked and foul means. Cybercrime is carried out by criminal individuals or criminal organizations.

Ebeleogu, Ojo, Adeh and Agu (2019) see cybercrime as a crime which involves the use of digital technologies in commission of offence, directed to computing and communication technologies. Cybercrime is mainly committed by our youths in order to make life earning easier thereby defrauding individuals or all organization of all kinds.

Ibikunle and Eweniyi (2013) in their own perspective describe cyber crime as the series of organized crime attacking both cyber space and cyber security. Cyber crime is now a tangled issue in Nigeria and the world at large; this is because many cyber criminals activities are being committed from remote sites which makes it difficult for Nigerians security agencies to trace those criminals.

The unavailability of recent laws on cyber crime makes it more difficult to handle the situation. Bosser, Adam, Berenblum and Tamer (2019) see cyber crime as a computer -oriented crime that involves a computer \and a network. The computer may have been used in the commission of a crime, or it may be the target.

Aghatise (2006) defined cyber crime as a crime committed on the internet using the computer as either a tool or a target victim. He identified four levels of cyber crime victims. They are the gullible, the desperados, the inexperienced and the unlucky people.

However, cyber crime is also seen as a type of criminal activity that either targets or uses a computer, a computer network or a networked device. These types of crime are mainly committed by cybercriminals or hackers who want to make money online the wrong way. Some cyber criminals are well organized, uses advanced strategies and are highly technically skill. Their goal is to make money and is usually done by individuals or an organization at large.

Cyber crime or computer-oriented crime is a crime that involves the use of a computer and a network. Computer is being used in the commission of such a crime. This may be on target or otherwise. Cyber crime may threaten a person, company or a nation's security and financial institution. There are numerous privacy concerns bordering cybercrime when secret data are intercepted or disclosed unlawfully or otherwise. Internationally, both government and non-state actors engage in cybercrime including espionage, financial theft, and other cross boarder crime. Cybercrime crossing international borders and involving the actions of a least one nation-state is sometimes referred to as cyber-welfare.

A report on cybercrime (sponsored by McAfee) published in 2014 estimated that the annual damage to the global economy was \$445 billion. Approximately \$1.5 billion was lost in 2012 to online credit and debit cards fraud in the U.S.A, in 2018, a study by Center for Strategic and International Studies (Csis), in partnership with McAfee, concluded that close to \$600 billion, nearly one percent of global GDP, is lost to cybercrime annually. From these authors review, one can conclude that cybercrime involves use of computer or computer based devices to defraud individuals or groups of individuals thereby acquiring unlawful financial status. The main interest of these fraudsters is to make money online through lies.

Ranges of Cybercrime

Cyber crime can be classified into the following categories:

Financial criminals or fraudster: this types of cybercrime involves phishing, scams, and it involves a level of social engineering as they require the criminals to pose as a reliable representative of an organization and commonly use it to defraud the victims banks phishing as a way of cybercrime involves hackers sending malicious emails attachments or URLS to users to gain access to their account or computer. This may also contain links to fake online banking or other websites used to steel private account information. Scams are usually in the form of ads or spams emails that include promises or rewarding of money. Internet scams includes enticing offers that are "too good to be true" and when clicked on can cause malwares to interfere and compromise information social engineering is a methods used by cyber criminals which involves lies and manipulation to trick people into revealing their personal information. This trick usually involves very convincing fake stories to lure victims into trap. Common social engineering attacks in the internet according to Ebeleogu, Ojo, Adeh and Agu (2019) includes

- I. sending victims an email that claims there is a problem with their account and he has a link to a fake website. Entering their account information into the site sends it straight to the cyber criminals (phishing)
- II. trying to convince victims to open emails attachment that contains malware by claiming it is something they might enjoy (like game) or need (like anti-malware software)
- III. Pretending to be a network or account administrator and asking for the victims password to perform maintenance.
- IV. Claiming that the victims has won a prize but must give their credit card information in order to receive it.
- V. Asking for a victim's password for an internet service and then using the same passwords to access other accounts and services since many people re-use the same password.
- Vi. Promising the victim they will receive millions of dollars, they, if they help out the sender by giving them money or their bank account information.
2. Website cloning: the most new system of cybercrime is the emergence of fake "copy-cat" web site that takes merit of consumers. What are uncommon with the internet or who do not know the main web address of the legitimate company that they are entering credit details in order to purchase goods from the intended company, instead unwittingly entering details into a fraudster personal database. The fraudster is then able to make use of the data at long run, either for his own advantage or to sell to others that have interest in committing credit card fraud.
3. Spamming: this refers to numerous amounts of emails being sent in order to promote and advertise products and websites.
4. Identify theft, credit card theft (phishy): this involves fraudulent electronic mails. it is the act of sending an email to user falsely claiming to be an established legitimate enterprise in order to scam the user into giving out his/ her private information that will be used for identify theft. Here, the criminals assumes to be the original person he//she stoles his or her identity.
5. Cyber harassment: this refers to electronically and intentionally carrying out threatening acts against individual. It also directs obscenities and a derogatory statements at a specific individuals focusing for instance on race, gender, religion, nationality, sexual orientation.

There are instance where a computer can lead to an enhanced sentence. In United States for instance, in the case of United States vs Neil Scott Kramer, the defendant was given an enhanced sentence according the US sentencing guideline manual & 2gi, 3(b) (3) for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of the minor to engage in prohibited sexual conduct". Krammer appealed the sentence on the grounds to convict him under this statute because his charge includes persuading through a computer device and his cellular phone technically is not a computer. Although Krammer tried to argue this point, the U.S sentence guidelines manual states that the term "computer means an electronic magnetic optical, electrochemical, or other high speed data processing device performing logical arithmetic's, or storage functions and includes any data storage facility or communication facility directly related to or operation in conjunction with such a device' in recent years, many countries of the world has enacted a law governing cybercrimes.

6. Cyber laundering: this is seen as an electronic transfer of illegally obtained monies with the goal of hiding its source and its destination too.
7. Hacking: in these categories of cybercrime, the hackers make use of the loop holes in operating system to destroy data and steal important information from victim's computer. This is usually done through the use of a backdoor program installed on one's machine. Hackers here, try to access to resource through the use of password hacking software hackers may also install many programs on someone programs without the persons knowledge. Such programmes may also be used to gain personal data like credit cards and passwords information.

Cyber theft: this kind of cybercrime is committed through the use of computers and communication system to steal data in electronic format or system. They crack into system of banks and transfer cash into their own personal bank accounts. This has been a major issue in the whole worlds because they transfer large amount of money to their personal account illegally. Organizations that are mostly defrauded usually keep quite because of fear of losing customers and shareholders.

This types of cybercrime is the regular cybercrime that individuals or organization mostly repot off they gain this money through little effort and this has negatively affected our youths as they believe in quick money syndrome.

Other classification of cybercrime includes worms and virus sending types, etc.

Methods of tricks employed by cyber criminals towards deceiving individual or organization in Nigeria

Nigeria as a country is so large to the extent that some individuals can go for a hide out for maximum period of a time which makes it difficult for security agencies to catch a cyber crime player. However, the following tricks are been used by the cyber criminals to maneuver peoples and collect their belongs;

- lottery scam: this is a type of trick which the scammer demands an advance-fee fraud which begins with an unexpected email notification, mailing or phone call (sometimes including a large check) explaining that someone have won" a large sum of money in a lottery. Here, the recipient of the message- the target of the scam- is usually told to keep the notice secret, " due to a mix up in some of the names and number', and to contact a "claims agent" after reaching the agent, the target of the scam will be directed to pay "process in fee" or "transfer charges"

so that the winning can be distributed, but will never receive any lottery payment. Many of these email lottery scammers use the original names of companies running lottery organization or other legitimate cooperation /companies, but this does not mean the original companies are into scammy business. Scam lottery email usually come from free email account such as Outlook, Yahoo, Hotmail, Live, MSN, Gmail, etc.

- Internet service time criminals, this has been developed by whiz kids in Nigeria. They do this by connecting cyber cafes to networks at some ISPs in a way that will not be detected the cafes to operate at no cost.

-bogus cashier's checks; in this kind, the victim showcase items for sale on the internet and is been contacted

- Internet charity: this is an e-crime common in Nigeria where cyber criminals host a websites of a charity organizations soliciting for monetary donations and materials to these companies that do not exist.

Next of kin scam: this kind of cybercriminals employs the means of collection of money from various banks and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative etc.

Causes of cyber crime in Nigeria as a country:

Nigeria as a multi-nation has faced with many challenges which have resulted in under development which affects Nigerian citizens negatively especially the youths as they are the people within the age range of labour force. The advent of computer has also contributed its own negative effect, which all these combined problems contribute to cyber crime.

Those causes are:

- Poverty alarming rate: Nigeria is regarded globally as a third world country due to high poverty rate index which is alarming. This poverty rate is increasing day by day, the rich are getting richer while the poor are getting poorer. Inadequate provision of basic amenities and an epileptic supply of power have put the small and medium enterprise into a pause.
- Peer group influence: this is usually showcased in certain environment where everyone wants to belong to a certain group or upper class without consideration of his / her background and this is grinding the moral upbringing of many youth in Nigeria. They try to emulate their mate in how to defraud individual and organization without consideration of its negative effect on them. All they want is that am driving life without the consideration that they say that "the ends justify the means"
- Negative role models and parental influence: this is caused by some parents who compare their children with other children that all they need from them is to make money whether good or bad. Money is all they want, money speaks. This usually lures these children into committing crimes.
- Security men collaborating with fraudsters: many security men and women instead of looking on how to arrest this cyber crime operator serves as body guards to them and covering them up in order to gain cash rewards. They go a long way to teach them the best way to invest this illegally acquired wealth without been arrested by government

security agencies and this has encourages this young men and women to remain in the crime.

- Corruption: Nigeria was ranked the third among the most corrupt countries in the whole world until 1999, when Nigerian created some financial crime monitoring agencies like EFCC (economic and financial crime commissions etc)

According to Ebeleogu, Ojo, Andeh and Agu (2019) the occurrence of a high economic condition and bad educational system also contributes immensely to the proliferation of cyber crime in Nigeria.

Other causes of cyber crime in Nigeria as a society include: high rate in urban migration, poor infrastructure, weak laws, and quick money syndrome.

Strategies for Reducing Cyber Crime in Nigeria

As they say, a problem seen is a problem half-solved. As the some problems identified in this paper include corrupt practices among citizens, quick money syndrome, high unemployment rate etc. The remedies to these can easily be suggested which include:

- Proper enlightenment / education, Nigerians government should try to be organizing regular seminars and workers to school leavers on how to survive with or without a befitting job. Here, the government needs to teach their citizens on proper use of internet security code to avoid cyber criminals cracking on their privacies.
- Enacting cyber security laws with a steady follow up to assist in monitoring the criminals.
- Job creation, government should create more job opportunities for the citizenry and also encourage small scale industries to operate by reducing their tax rate and giving them grant and loans
- Fire walls, this protects a computer system from unauthorized access. Network farewells may be hardware devices, software programs, or a combination of the two.
- Address verification system (AVS), this could be used in ensuring that the address entered on your order from for people who receives parcels from other countries matches the address where the cardholders billing statement are mailed from to avoid defrauding the individual.
- Creation of more skill acquisition centers, Nigeria government need to create at least one skill acquisition center in every local government development centers to enables may access the opportunity of learning a skill. This skill if learned by the youth will go a long way in reducing cyber crime in Nigeria
- Proper implementation of cyber security laws; information technology security or cyber security is the protection of computer system and network from information disclosure, theft or damage to their hardware, software or electronic data as well as from the disruption or misdirection of the service they provided, in order for government to proper implement this, all security needs to employ expert in the field of cyber security in the field of cyber security to avoid poor porous internet working

Conclusion / Recommendations

Nigeria as a country is being regarded as a ridicule due to high rate of corrupt practices whose one example is cyber crime activities. These criminal activities bring about reputation loss to a nation, financial loss, low productivity, etc. And these consequences are glaring in Nigeria. Based on these findings, the paper recommends:

- Proper execution of cyber security laws the country by various levels of government from federal, state down to local government for easy checkmating of these fraudsters and their agents.
- Seminars and skill acquisition centers should be created by the government to reduce unemployment rate.
- Individuals should also play their part by avoiding any suspected fraudster alert like fake bank alert and also maintain privacy of any of their password in the internet.
- Grants and loans should be given to individuals and small scale industries to direct their interests into working to earn a better living than being engaged in cyber crimes.
- Churches leaders, Muslims faithful and practitioners of African Traditional Religion should preach against illegal ways of making money to the adherents of their respective religions.

References

- Adebusuyi , A (2008) The Interest And Emergence Of Yahoo Boys Sub-Cultures In Nigeria, International Journal Of Cyber Criminology 0794-2891, Vol 2 (2) 368-381, July – December
- Aghatise, E.J (2008) Cybercrime Definition. Computer Research Center, Retrived from [Http://Www.Crime-Research.Org/](http://www.Crime-Research.Org/) Article Joseph 06/2
- Aghatise, E.J (2006) Level of Awareness of Internet Intermediaries Liability. Unpublished HND Project, Auch Polytechnic, Auch, Edo State Nigeria.
- Ajibike, T (2019) “Youth and Cybercrime In Nigeria, Punch News Paper March 15.
- Bossler Adem, Berenblum, Tamar New Directions In Cybercrimes Research Journal Of Crime And Justice 42 (5), 495-499: Doi:10.1080/0735 648x. 2019.1692426.Issn 0735-648x
- Ebeleogu, C.U, Ojo, S.D. Andeh, C.P And Agu, E.O (2019) Cybercrimes, Its Adherent Negative Effects On Nigerians Youth And The Costly at Large, Possible Solution. International Journals of Advances in Scientific Research and Engineering (Ijasre). E-Issn: 2454-8006, Volume 5, Issue 12, December 2019.
- Ibikunle , F. And Eweniyi .O (2013) Approach to Cyber Security Issues in Nigeria, Challenges And Solutions (Iycrsee) International Journal Of Cognitive Research In Science, Engineering And Education Vol.1no.1.2013
- International Telecommunication Union Retrieved From [Http:// Www. Itu,Int/En//Pages /Default .Aspx](http://www.itu.int/en/Pages/Default.aspx).
- Longe, O.B, Chiemeka .S (2008); Cyber Crime And Criminality In Nigeria- What Roles Are Internet Access Points In Playing European Journal Of Social Science – Volume 6, Number 4
- Nkenga, E. (2008) Combating Cyber Crime Menace in Nigeria Retrieved On 15th January 2012 From This Day .[www. allafrica.com](http://www.allafrica.com)
- Olumide, O.O. and Victor, F.B (2010) Crime in Nigeria. Trends, Tricks and Treatment. The Pacific Journal of Science and Technology Volume ii. Number 1 2010 (Spring)
- Stassman. P.A. (2009); Cyber Security for the Department Of Defense, Retrived July 10, 2011 from [Http://Www-Strassman.Com/Pubs/Dod/Cybersecurty-Draft](http://www-strassman.com/Pubs/Dod/Cybersecurty-Draft) -Vipdf.