PalArch's Journal of Archaeology of Egypt / Egyptology

THE ANTICS AND TACTICS OF CYBER FRAUDSTERS IN NIGERIA: THE NEED FOR COUNSELLING INTERVENTION FOR ATTITUDINAL CHANGE

Effiom, Bassey Ekeng[1], *Undiyaundeye, Florence A*[2]

[2]Department Of Guidance and Counselling, Faculty of Education University of Calabar - Nigeria

Email: [1]Drbasseyekeng111@gmail.com

Effiom, Bassey Ekeng, Undiyaundeye, Florence A. The Antics and Tactics of Cyber Fraudsters in Nigeria: The Need for Counselling Intervention for Attitudinal Change -- Palarch's Journal of Archaeology of Egypt/Egyptology 18(08), 2426-2432. Issn 1567-214x

Keywords: Cybercrime, Internet Fraudsters, Account Hacking, E-Banking

ABSTRACT

Social engineering is a tactic used by cyber criminals that used lies and manipulation to trick people into revealing their personal details and information. 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 resulting in exploitation and crime. Some of the antics and tactics cybercriminals use to commit crimes may include Botnet, Drug's trafficking deals, DDoS attacks, Cyber-stalking, Scammers, Cyber- terrorism and pop – ups. Some of the immediate causes of cybercrimes includes Parent influence / negative role models, Poor remuneration from law enforcement agencies, Non enforcement of cybercrime laws, Urbanization, Security forces collaboration with Fraudsters and the quest for quick Wealth : some of the strategic counselling approaches to forstall cybercrime may include *terminate online session completely*, *create backup of important data*, *avoid phishing emails*, use security programs, protecting your password, participation in social networking and the use a two-step-authentication

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 centre data system , theft, child

pornography built image, online transaction fraud, internet sales fraud and also deployment in internet malicious activities such as virus, worm and third party abuse that like phishing , email scams etc. The universal approach of network like internet at all level of network need to recover from committing illegal activities 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. Notably, cybercrime is of different classes in Nigeria; the form the range of yahoo boys and their 419 internet frauds; hacking; software piracy; phonograph; credit score card or ATM fraud; denial of service attack; virus dissemination; phishing; cyber plagiarism; cyber-stalking; cyber – defamation.

Overview Of Cybercrime

Before delving into the term '' cybercrime'' it is pertinent to define the team fraud. In law, fraud committed by a fraudster as an international deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud can violate civil law (e.g a fraud victim may sue the fraud perpetrator to avoid the fraud or recover monetary compensation) or criminal law (e.g a fraud perpetrator may be prosecuted and imprisoned by governmental authorities), or it may cause no loss of money, property, or legal right but still be an element of another civil or criminal wrong (Nkanga, 2008). The purpose of fraud may be monetary gain or other benefits, for examples by obtaining a passport, travel document, or driver's license, or mortgage fraud, where the operator may attempt to qualify for a mortgage by way of false statement. Another word for fraud is 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 forms different angel than the others. 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 judgement, crime is concomitant with destruction and carnage. the cybercrime may be broadly classified into three groups these 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 following groups:

i. Against individuals: (a) harassment via election mail (b) dissemination of obscene materials (C) cyber – stalking (D) defamation (e) indecent exposure (f) cheating (g) unauthorized control / access over computer system (h) email spoofing (i) fraud.

ii. Against Individual Property: (a) computer vandalism (b) transmitting virus (c) authorized access / control over computer system (d) intellectual property crimes (e) internet thefts
iii. 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.
iv. 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.

Antics and Tactics of Fraudsters

Before the internet, criminals have to dig through people's trash or intercept their mail to steal the personal information now that all 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. most cybercrimes are committed by individuals or smalls groups. however, large organized crime groups also take advantage of the internet this ''professional'' criminals find new ways to commit old crimes, treating cybercrime like a business and forming global criminals' communities. criminals' communities share strategies and tools and can combine forces to launch coordinated attacks the even have an underground marketplace where cyber criminals can buy and sell stolen information and identities.

Social engineering: social engineering is a tactic used by cyber criminals that used 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 attack include.

a. 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 sent it straight to the cybercriminal (phishing).
b. 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).
c. Pretending to be a network or account administrator and asking for the victims to perform maintenance.
d. Claiming that the victims has won a prize but must give their credit card information in order to received it.
e. Asking for a victim's password for an internet service and then using the same password to access other account and services since many people re-use the same password.
f. Promising the victims they will receive millions of dollars, if they will help out the sender by giving them money or their bank account information.

Attack Techniques

Here are few **Tactics** of attacks cybercriminals use to commit crimes. you may recognize a few of them:

a. Botnet – are networks from compromised computer that are controlled externally by remote hackers then send spam or attack other computer through these botnets. botnets can also be used to act as a malware and perform malicious tasks.

b. Drug's trafficking deals - another form of cybercrime technique is drugs-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 advantages of the internet to sell their illegal substances through encrypted e-mail and other internet technology. These virtual exchanges allow more intimidated individuals to make comfortably purchase of illegal drugs.

c. 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 down by overwhelming the site with traffic from s variety of sources, large network by overwhelming the site with traffic from a variety of sources large network of infected devices known as botnets are created by depositing malware on users'' computers. The hackers then hack the system once the network is down.

d. Cyber-stalking – this kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and email s typically cyber stalkers use social media, website and search engines to immediate a user and instil fear. usually, the cyberstalked knows their victim and make the person feel afraid or concern for their safety.

e. 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 restaurant when the card is out of the owner's view ,and frequently the credit card information is now sold online through a criminal community .this cybercrime occurs when a criminal gain access to a user's personal information to steal fund , 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 plane criminal's activity and claim government or bank benefit 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.

f. Cyber- terrorism – a cyber terrorism 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 network .the aim of a cyber terrorist is chiefly to intimidate government or to advise his or her political or social objective by launching various attacks against computer , network , and the information stored on them it means that any act intended to instil fear by accessing and distorting any useful information in organization or government bodies using computer and internet is constitute cyber terrorism.

g. Pups- pups or potentially unwanted programs are less threatening than other cybercrimes, but are the types of malwares. they uninstall necessary software in your system including search engines and pre- downloaded apps. they can include spyware or adware, so it's good idea to install antivirus software to avoid the malicious download.

Root Causes of Cybercrime Amongst Youth and The Society in Nigeria

With the huge and increasing population of Nigeria which presently stand at over 200 million, we look at the major causes of cybercrime among the youth and society at large.

a. Parent influence / negative role models – youths are mirrors of the society, but it is quite unfortunate how parents neglect their restful duties. besides, it's miles saddening to look at the many parents transmit crimes values to their wards, through socialization as if it is a social and cultural
Value which ought to be transmitted to the younger generations the bad role version syndrome is having devastating effects on the lives of the youngsters related to in cybercrimes and other sharp practices (make, 2012) remarked that today many parents transmit crime values which ought to be transmitted to the younger generation.

b. 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 effc (economics and financial crime) Commission and the icpc (independence corrupt practices commission) but money recovered has not been injected by economy judiciously used for the benefits of the benefit of the citizenry. it is also noticed that most of the agencies have cybercriminals on their payroll and such make it very difficult to identify them and this in point makes it impossible tpo arrest and convict them.

c. Weak implementation of cybercrime laws and inadequate equipped law agencies the Nigeria legislation must implement strict laws regarding cybercriminals and when criminal offences occur, perpetors must be punished for the crime they have committed because cybercrime reduces the nation's competitive edge, failure to prosecute, cybercriminals, can take advantages of the week 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. Unfortunately, the nation is not well equipped with sophisticated hardware to track down virtual forensic criminals. Laura (2012) state the '' African Countries have been critized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equippeprivate sector is also lagging behind in cubing cybercrime'' Nigeria is not and exception this rule.

d. Urbanization : urbanization is one of the causes of cybercrime in Nigeria ; it is the massive movement of people from rural settlement to cities .according to Wikipedia urbanization is looked at the massive physical growth of urban areas as the 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 elites find it lucrative tom invest crime of cyber because it is a business that requires less capital to invest and they are popularly called ''yahoo boys '' as such the elites amongst them find it lucrative to invest in the cybercrime because it is a business that requires less capital.

e. **Police Collaborating with Fraudsters:** the Nigeria 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 woman see the Yahoo Boys (Cyber Fraudsters) as an avenue of making quick cash even when the 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 book are seen

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

f. **Quest Of Quick Wealth**: Another cause of cybercrime 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.

Basic Counselling Tips to Get Protected from Cybercrime

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

a. *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 '' logout or sign out'' button. Avoid using the option of '' remember'' your username and password information.

b. *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.

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

d. 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 to kind of security programs installed.

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

f. 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 setting to prevent personal information being broadcast.

g. 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.

CONCLUSION

Nigerian has lost so much reputation and bilateral trade options from foreign nations. The businesses and investment which was supposed to get into the country goes away because of the huge presence of 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 obvious that cybercriminals cannot be easily eliminated, but it can certainly be minimized. With the collaborative efforts of all stakeholders like individuals, corporate organization and government to nip the scourge in the bud. Government to also in respect levels ought to ensure that its legal guidelines practical cybercrimes. It is vital that Nigeria as a nation takes measures to make sure that its penal and procedural laws are adequate fulfil the challenge posed with the

REFERENCES

Aghatise, E. J. (2006). Cybercrime Definition. Computer Research Centre, Retrieved from Http://Www.Crimeresearch Org/Articles/ Joseph06/2

Ajibike T. (2019) Youth and Cybercrime in Nigeria'', Punch News Paper, March 15

Aransiola, J, & Asindemade, S. (2011). Understanding Cybercrime Perpetrators and The Strategies the Employ in Nigeria. Cyber psychology, Behaviour, And Social Networking ,14 (12) Pp.

759-63

Cooper, A, McLaughlin, I.P.& Campbell, K.M (2000) Sexuality in Cyberspace: Update for the 21st Century. Cyberpsychology & Behaviour Vol.34, Pp.521-536.

Longe, O.B., & Chiemeke, S.C. (2008). Cyber Crime and Criminality in Nigeria – What Roles Are Internet Access Point Playing? European Journal of Social Sciences, 6(4), Pp.132-139.

Meke S.E.N. (2012): An Article '' Urbanization and Cyber Crime in Nigeria: Causes and Consequences''.

Nkanga, E. (2008). Combating Cyber Crime Menace in Nigeria. Retrieved On 15th January 2012 from Thisday.Www. Allafrica.Com

Reddick, R., & King, E. (2000). The Online Student: Making the Grade on The Internet. Fort Worth: Harcourt Brace.

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.