PERENNIAL CYBER CRIME AMONG TERTIARY INSTITUTION STUDENTS : CASES CLASSES CAUSES AND CURE

Adewusi A Gregory, Lagos State University, Nigeria

+2348030888507

gregade2000@yahoo.com

&

Samuel Akinyemi , Lagos State University, Nigeria

+2348083885784

akinyemisam2006@yahoo.com

Abstract

It is no longer strange that major culprits of cybercrime are the highly sophisticated intelligent youths in our various institutions of higher learning .Findings of different shapes indicate that Internet fraud in tertiary institutions are socially organized and highly networked. The act involves nefarious networking of fellow fraudsters and bank staff in most cases. Victims pay money through domiciliary accounts, cheques, credit cards, Money Gram and Western Union .In 2003 alone, an estimate of $13 billion to $226 billion was lost to cyber attacks. No doubt the impact of this colossal loss is significant globally .Cyber crime is reported to be profitable at meeting financial exigencies of paying school fees, acquiring properties and sustaining living. This informal network will continue to impede sincere attempt to curb cyber-criminality in Nigeria. The Government must create an enabling environment that will dispel the immanent fear of unemployment youth face after schooling, check unbridled corruption, and integrate moral values into the body polity. Against this background, this paper pre occupies itself with cases and classes of internet frauds with the aim of examining the remote and immediate causes and proffering logical solutions minimizing the social misdemeanour if not totally curbed.

Keywords:, Intellectual, Cyber Crime, Tertiary Institution

Introduction

Computer crime can be broadly defined as criminal activity involving 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), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (or identity theft) and electronic fraud.

According to Aghatise (2006), it is alarming that 80% of cyber crime perpetrators in Nigeria are students in various 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 (Tade & Aliyu, 2011). This act is painting Nigeria black in both national and international market.

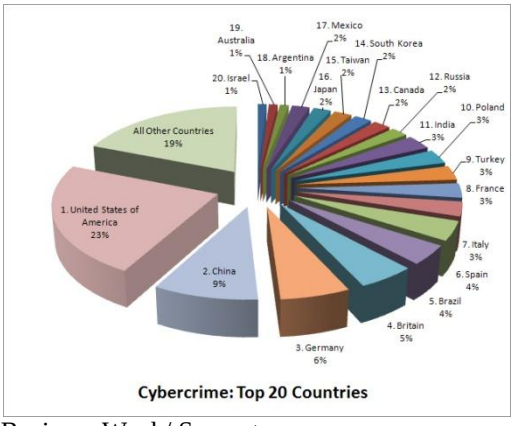
Numerous crimes are committed on daily basis on the internet with Nigerians at the forefront of sending fraudulent and bogus financial proposals all over the world (Longe & Chiemeke, 2008). According to a 2007 internet crime report released by the Internet Crime Complaint Centre (IC3), Nigeria ranks third among cyber crime committing countries in the world. The report indicates that the "Nigerian letter fraud" (Email Scams) received in the United States, constituted 1.1% and the individuals reporting fraud-type monetary loss in 2007 puts Nigerian letter fraud at 6.4%, amounting to 1,922.99 million US dollars (Odapu, 2008).
From research findings cyber crime is not peculiar to Nigeria as other counties of the world have their shares.

CASES OF CYBERCRIME

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 centre. 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.
On recent internet scam case was reported on the Sunday PUNCH newspaper of 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.



Source: Business Week/ Symantec

America has the largest share of 26% cybercrime world over followed by other countries with 19% which Nigeria belongs. Other countries also have cymbal criminals in them as seen above.

CLASSES OF CYBERCRIME

Crime comes in different forms and the perpetrators are constantly devising new ways of conducting their nefarious acts. The forms considered below are not meant to be exhaustive but they are meant to portray some of the different taxonomies of e crime.

Hacking

This is a general term for e crimes like illegal access, defacing, hijacking, bombing, denial of service attack, super zapping, eavesdropping, etc. Some Internet users think that hacking is harmless fun and even quite clever, but it can be a serious invasion of privacy and a significant threat to e commerce.

Cyber Terrorism:

Parker (1983) defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. 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. Another form of cyber terrorism is cyber

extortion a form of cyber terrorism in which a website, e-mail server, computer systems is put under attacks by hackers for denial of services, demanding for ransom in return.

Fraud - Identity Theft:
Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone. For instance, making a false bank webpage to retrieve the account information of someone. The concept is simple; someone gains access to your personal information and uses it for his own benefit. In Nigeria people design web links forms requesting users to fill in their basic information including, unique details like pin numbers and use that to commit crimes.

Drug Trafficking Deals:
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.. 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 (www.wikipedia.com)

Malware:
Malware refers to viruses, Trojans, worms and other software that gets onto your computer without you being aware it's there. When such software is downloaded, it infects the computer system and destroys valuable information. The Trojan horse is also a technique for creating an automated form of computer abuse called the salami attack, which works on financial data. This technique causes small amounts of assets to be removed from a larger pool. The stolen assets are removed one slice at a time.

Spam:
Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam and so on (Saul, 2007).

Yahoo plus
A new phenomenon in cybercrime is mixing spiritual elements with internet surfing to boost cybercrime. The methods used include *ase or mayehun* (incontrovertible order), charmed or magical rings (*oruka-ere*) and incisions made around the wrist, which are used to surf the net, while *ijapa* (tortoise) is used to navigate profitable sites. Unsuspecting victims fall under the spell of the *ase* via phone conversation where spiritual orders are made to the victims without their objecting.

Logic Bombs
A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display any object on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in with viruses.

CAUSES
The Nigerian population census in 2006 reveals that Nigeria is a country with about 160 million people. This write up discusses some of the reasons that may cause cyber crime in Nigeria.

Urbanization is one of the causes of Cyber crime in Nigeria; it is the massive movement of people from rural settlement to Cites, **Unemployment** is another issue as Nigeria is saddled with almost 20 million unemployed people, **Quest for Wealth** is another cause of cyber crime, **Inefficient Cyber Crime Laws** is not helpful to curbing cyber crime and **Negative Role Models** where youths tend to emulate wrong models in the society is the order of the day (Meke ,2012).

CURE

Recommendation.
Individuals should be cyber crime conscious by ensuring proper antimalware protection on their computer systems, never to share their Personal Identification like Number(PIN), bank account, email access code to unknown persons, Governments should assure that their laws apply to cybercrimes. African countries are bedeviled by various socio economic problems such as poverty, AIDS, fuel crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cybercrime. Nevertheless, it is important that Nigeria as a nation take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. Making available basic infrastructure and social amenities by the government will to an extent reduce economic

hardship of people and make them to embark on profit oriented life style rather than look for fast method of making money at the determent of the society. More importantly, the government should discourage incessant strike of tertiary institution teachers so that the youth are not left idle to think of cybercrime to engage them.

REFERENCES

Aghatise, E.J (2006): Cybercrime Definition. Computer Crime Research Center. June 28, 2006.
Laura Ani (2012): "Cyber Crime and National Security: The Role of the Penal and Procedural Law.
Regulations. Hershey, PA, USA:IGI Global. ISBN 978-1-60960-830-9.
Mbaskei Martin Obono (2008): Cyber crimes: Effect on Youth. org accessed 27 February, 2013
Meke Eze Stanley, N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".
Parker D (1983): Fighting Computer Crimes, U.S. Charles Scribner's Sons.
Saul Hansell,(2007): Social network launches worldwide spam campaign, New York Times.
Tade O., & Aliyu, I. (2011). Social Organization of Internet Fraud among University Undergraduates in Nigeria International Journal of Cyber Criminology, 5
(2), 860–875