Journal of the Nigerian Association of Mathematical Physics
***Volume27*, (*July, 2014*), pp 471 – 478**
© J. of NAMP

Cybercrime and Its Impact on the Youth

[1]Osagie, S. U. M. and [2]Obahiangbon K.O.

Department of Mathematics and Computer Science,Benson Idahosa University,
Benin City, Nigeria.

Abstract

The internet offers numerous advantages in today's changing world. Most glaring is the transactions (Local or International) embarked on by people on a daily basis. Knowing that internet is a collection of segmented (local) networks linked together by a common purpose for sharing resources or information and being a borderless society crime easily spreads from one country to another leaving the end users at risk. Most cumbersome is the lack of legal standard to combat this illicit act due to diversity in traditions, culture and religious beliefs of end users. It is therefore paramount to have idea of what happens online during such transactions, especially with respect to insecurity(Cybercrime) and the impact on the Youth. This research isaimed at looking into the impact of cybercrime on the youth and the measures employed in avoiding crime when surfing. A survey was conducted in Benin City, Nigeria, using a questionnaire to obtain a valid result on its awareness and 97.1% of the sampling data revealed that there were no legal actions taken in combating and restoring hope to the youth who have their data invaded by intruders/crackers.

Keywords: Illicit, Combating, Surfing, Cybercrime and Misrepresentations.

1.0 Introduction

Internet as the name sounds is a platform that enables thousands of individuals to interact, make transactions, share resources etc. In this 21st century the word cybercrime is no longer news, this is what some persons not educated in this part of Nigeria (Benin City) called "Yahoo Yahoo". Everybody using internet in today's changing world must find a way to cope with this menace perpetrated by criminals online. Cyber Crimes and proliferation of Yahoo Addicts is a product of a recent technological advancement leveraged by the phenomenon of globalisation [1].Over the past twenty years, unscrupulous computer users have continued to use the computer to commit crimes; this has greatly fascinated people and evoked a mixed feeling of admiration and fear [2].Cybercrime is a crime committed via cyberspace leading to several damages to people's properties. The crime began with disgruntled employees causing physical damage to the computers they worked with, with the aim to get back at their superiors. As the ability to have personal computer at home became more accessible and popular, cyber criminals began to focus their efforts on home users[3]. A research from the same author made known the history of the first published cybercrime in 1960s [3]. Today it is no more a crime committed inside it has found its tent in the domestic home of personal Computer (PC) users; it also focuses on digging into companies'data and

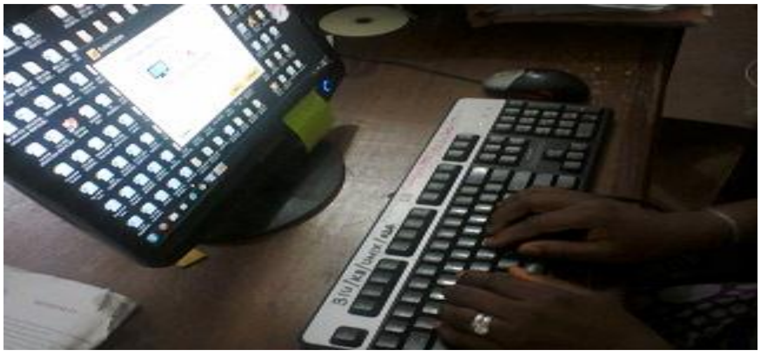

Figure 1: Pictorial View of a Cyberspace User

Corresponding author: Osagie, S.U.M.E-mail:osagiescalemax@yahoo.com,Tel.: +2348036324156

government's activities with the aim of stilling important information or data and disregarding the philosophical foundation of information technology gargets. According toMaitanmiOlusola,Ogunlere Samson, Ayinde Semiu, Adekunle Yinka in [3] categorised cybercrimeinto three and they are

- Crimes against persons.
- Crimes against Business and Non-business organizations.
- Crimes against the government

We are of the view that Nigeria as a country lacks the capacity in combating crime within the cyberspace due to poor funding and youth haveembarked on self help in navigating their way via internet. In Benin City there is no structure by government or corporate bodies in checkmating these illicit activities committed on the internet. Lack of funding in educating PC users in this part of the country (Benin City) has become norm and this has continued to have negative effect on the Youth living within Benin City.

2.0 The Objectives of this Work

Cybercrime has come to stay and the earlier individual, Corporate Bodies andGovernments become conscious of this the better for us. The objectives of this work is to ascertain the level of awareness of cybercrime amongst the computer users (Youth)within Benin City, and to identify the Measures taken in combating this illicit act presently wreaking havoc on the cyberspace and the Benin Youth. It is our desire that Edo State government will march words with actions to ensure measures are put in place to enlighten the Youth of this crime and the need why they should be more vigilant than ever and create programmes that will encourage, train, and upgrade the law enforcement agencies ability in combating the systematic trend of these criminals. Some recommendations were proffered to help reduce or eradicate this illicit act

3.0 Overview of Cybercrime

Cybercrime:

In understanding the indebt meaning and definition of cybercrime let's look deeply into the traditional crime committed by hoodlums, taking the issue of community's lands as a case study.Killing of people and destroying of propertiesare crimes government and traditional rulers have no control over and the increase is on the rise living individual owners ofland at risk. If examined critically from the introductions it was stated that cyberspace is a borderless society and if governments, cooperate bodies are faced with problem in maintaining peace and order in some communities with boundaries how much more a cyberspace that has non limit to which you can go.

Figure 2: Cyberspace, a borderless society

4.0 "Cyber and Crime"

What is CYBER: According to the oxford advanced learner's dictionary six editions define cyber as "connected with electronics communication, especially the internet and defines" a **CRIME** as "an activity that involves breaking the law: an increase in violent crime or an illegal act or activity that can be punishable by law".

'Definitions' of cybercrime mostly depend upon the purpose of using the term. A limitednumber of acts against the confidentiality, integrity and availability of computer data or systemrepresent the core of cybercrime. Beyond this, however, computer-related acts for personal orfinancial gain or harm, including forms of identity-related crime and computer content-related acts(all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily toefforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the coreof cybercrime acts. However, a 'definition' of cybercrime is not as relevant for other purposes, suchas defining the scope of specialized investigative and international cooperation powers, which arebetter focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime'construct.[4]

In this work we shall define Cybercrime as a violation of the procedural act of obtaining a validdata/information online from an authorised owner or user with the aid of computer/electronic garget by way of misrepresentation (caricature).

4.1 Elements of Cybercrimes

Cyber crime share three elements that enable it function in cyberspace and five topmost crimes committed in cyberspace are listed bellow[5, 6]

Elements

1. Tools and techniques to perpetrate a crime
2. Approach or methodology for executing the criminal plan known as a vector
3. Crime itself that is the end result of those plans and activities (a cybercrime is the ultimate objective of the criminal's activities)

Five Topmost crimes in Cyberspace

(1)Tax-Refund Fraud: (2)Corporate Account Takeover: (3)Identity Theft: (4)Theft of Sensitive Data: (5)Theft of intellectual property

4.2 Impact of Cybercrime In View

The flexibility internet has brought to our door stepsis what is bridging the divided world of information today; its impact will continue to either have a positive or negative effect on the end users. The original purpose of the internet is to bridge resources that are culturally divided around the globe and people still regard this importance of cyberspace but the question of using it to bridge resources has led to diversity in usage by various people. To some it is a platform to actually make the real thing done while to some it is a world that is free to commit all source of atrocities because of its borderless nature. Its impact has come to stay and it will continue to play its role in today's changing world of information and IT equipments. As the world advances in technology it is also common to know that there will be new strategies employed by cyber criminals to ensure they remain on the game. Therefore, corporate bodies, individuals and Governments in particular should ensurereorientation of the public to this criminal act and the need for the public to stand firmlyin defending their right. Since governments are the ones saddled with theresponsibility of providing gargets to law enforcement agencies to combat crime they should make adequate laws and follow it upwith the political will (implementations) to ensuring perpetrators are brought to book and adequate sanctions are taken so as to discourage others already bracing their chest.

4.3 Some Common Crimes in Cyberspace

Yahoo Yahoo: Chapter 39, serial number 419 of the criminal code actstates that any person who by any false pretence and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any other person anything capable of being stolen, is guilty of a felony, and liable to imprisonment for three years [7, 8]. Yahoo yahoo as it is popularly called in Benin City falls on the purview of 419. Since the introduction of this crime it has found it foot in the domain of Benin youth surfing internet. They regard the section of the Nigeria criminal act as nothing, following the level/nature of penalty/punishment for the offence.

Pornography: This involves the use offilms; video and pictures in portraying human nakedness,thus, leading to human sexual organs responding accordingly when viewed or seen and many are now using it to commit all sorts of illicit act because the internet has helped to promote it

Virus: Computer Virus is malicious in nature and it is an infectious program that has the ability to replicatewhen in contact withtransferable garget. It executes itself in a file unsuspectinglyto the person transferring data

Phishing: These are illicitmails asking for users electronics update. These include email username, password, phone numbers, and credit card details in a website basically designed to commit crime.

Spoofing: This is aclever act of cybercrime they create/establish protocol Packet and this is carried out by an intruder by way of using somebody else's IP addresses. They always stand pretentious at the middle of two end points of network that has two users accessing or interacting online.

Software piracy: If there is anything or issue a programmer faced is the rate at which people reproducesand marketsoftware not originally produce by them

Denial of service attack: This is an act committed by intruder (attacker) to preventing authorised persons or a legitimate system owner of not been able to use the system or network and they do this by down pouring (flooding) a network or disrupting a network to make the legitimate users have no access

Cyber defamation: Chapter 33, serial number 375 of the cited material states the punishments for any person found or aiding the publication of defamatory matters and this ona wide range in the cyberspace. Though it is not a criminal act but it involves the use of words or statement that brings down the reputation of others or eminent persons [8]

Cyber terrorism: This part of cyber crime is gaining more friends because conflict has become the bedrock of different nations**.** According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[9]

Hacking/Cracking: When the definition between a hacker and a cracker seems cloudy to you remember to look at motivation. A true hacker is a tinker, one with a curious mind; they push to the limits and take things apart in order to further their own understandings.

The Cracker may be teaching himself to do more too, but his motive is to use what he learns, to exploit weaknesses and to do harm. Where the hacker is an explorer, the cracker is an exploiter. The hacker explores and takes notes, while the cracker explores and takes advantage. Hackers don't leave tracks. About the only changes they make to any systems they get in to change the logs to hide that they got inside. Crackers are the ones who delete files, make changes, and generally need to show off that they finally managed to enter a machine. [10]. though, there are certified hackers, there duty it to help track these criminals in well established IT firm.

Plagiarism: This is an act of stealing someone else's intellect or idea without making reference /citing the original owner of the idea. This is covered under the intellectual right act

4.4 Data Analysis

The administered questionnaire has alphabets representing the view of the Youth. A to Z and AA to AF represent the entire survey respectively and these are the key to Table 1.

Table 1: Analysis Table

S/N	A	B			
1, 3, 6, 7, 9 and 12	Yes	No			
2	C	D	E		
	Personal	Business	Both		
4	F	G	H		
	Several Times Per Day	Everyday	Several Times Per Week		
	I	J	K		
	Once a week	Several times per month	Once a Month		
5	L	M	N		
	Avast antivirus	Adaware	Firewall		
8	O	P			
	Online Banking	Shopping (Ebay.com etc)			
	Q	R	S		
	Research and general information	Email instant messaging	Only for work		
10	T	U	V	W	
	Viruses	Spyware/Adware	Hackers	Indifferent	
11	X				
	Per to per Network				
	Y	Z			
	Freeware Programs	Surfing			
13	AA	AB	AC	AD	AE
	Data Collection by Hackers	Web Defacing	Server Hijacking	Denial of Service	An attack happened
14	AF				
	No Option				

Table 2: Result Table: Tabulated Data

S/N	Samples	Specifications	Rated Samples	%
1	**Internet Users**			
		A	397	99.25%
		B	03	0.75%
2	**Purpose for Using Computer**			
		C	180	45%
		D	50	42.5%
		E	170	12.5%
3	**Device Availability To Internet**			
		A	375	93.75%
		B	25	6.25%
4	**Frequent Nature Of Internet**			
		F	100	26.67%
		G	200	53.33%
		H	29	7.73%
		I	05	1.33%
		J	21	5.61%
		K	20	5.33%
5	**Program For File Protection When Surfing Internet**			
		L	362	96.5%
		M	02	0.5%
		N	05	1.3%
		L & N		1.6%
6	**Are These Programs Updated**			
		A	255	68%
		B	120	32%
7	**Do You Download**			
		A	193	52%
		B	180	48%
8	**Purpose Of Using Internet**			
		O	05	1.33%
		P	20	5.33%
		Q	79	21.1%
		R	30	8%
		S	10	2.67%
		Q & R	231	62%
9	**Use Of Credit Card As A Means Of Payment Online**			
		A	100	3.54%
		B	257	72%
10	**Threat Encountered**			
		T	301	80.3%
		U	0%	0%
		V	50	13.33%
		W	24	6.4%

11	**Where Did They Come From**			
		X	05	1.423%
		Y	20	5.7%
		R	72	20.51%
		Z	201	57.3%
		W	53	15.1%
12	**Has Your Company Or You Been Attack Via Internet**			
		A	309	82.4%
		B	30	8%
		W	36	9.6%
13	**What Kind Of Attacks Were They**			
		AA	60	19.42%
		AB	20	6.47%
		AC	18	5.83%
		AD	199	64.4%
		AE	12	3.88%
14	**Option/actions Use In Prosecuting The Incident**			
		AF	300	97.1%
		W	09	2.91%

Following the sectional analysis of the administered questionnaire, 1-4 illustrates how friendly Benin youth are with internet. The first raw (s/n 1) with A=99.25% confirmed almost all youth living in Benin City have internet access and this is a positive impact, it means most youth within the City has internet knowledge. WithB=0.75%clamingignorant of internet knowledgeshows the truth following the current trend of social media.Though, not captured in the questionnaire openly the purpose of (s/n 2) was to ascertainwho uses computer most between Personal and Businesses or even both. The result gotten revealed that computer had wide rage in personal usage among the youth with C having 45%, D having 42.5% this means 2.5% is the difference between thetwo users. This should be close to the truth because youth are more found with personal computer compare to adult and what they do withit is endless. For breakdown of the remaining percentage for1-4 columns see the table 2.

Column 5 -9 in the analysis table gave insight to what actually happen whenever the youth are on a cyberspace, and the program use in protecting data and computer. The results gotten from (s/n 6) column 6 shows the regular nature of the software update and this is a fantastic impact on the youth. Avast antivirus is having upper hand in itsusage; this means youth in Benin know how dangerous internet might be. With L= having 96.5%, M=0.5%, N=1.3% and L&N=1.6% tells the awareness of criminal act ravaging the internet world because they fully understood, but with s/n 6B having 32% it means some internet users (youth)in the state are still vulnerable to this crime committed online and following the percentage itmeans there are enormous task still awaiting the governments and individuals in eradicating this illicit act. For breakdown of phase 2 see the table 2

The third phase which is column 10-14 sampled the challenges face by the Benin youth when on cyberspaceand it is interesting to know that even with the knowledge ofcrimescommitted on the internet many still have their system or data invaded. T shows that over 80% have their system or data affected by viruses and 13.33% have their systems or data hacked by intruders. With 82.2% saying both themselves and their company have been attacked it means this crime is having an effect amongst the youth. This is a worrisome act that has found its ground in Nigeria and if adequate steps are not taken it might cripple the city economy. This is seen from the s/n 14 column with AF having 97.1% of no legal action taken against the perpetrators, and it is an indication that there is no adequate laws strong enough to trap down these criminals and it goes further to unveil the inability of the agencies saddled with the responsibility of combating this crime, in this case we referred to the Economic and Financial Crimes Commission (EFCC) but they are also restricted by the Nigeria constitution or laws on cybercrime. For breakdown of this phase see analysis table 2.

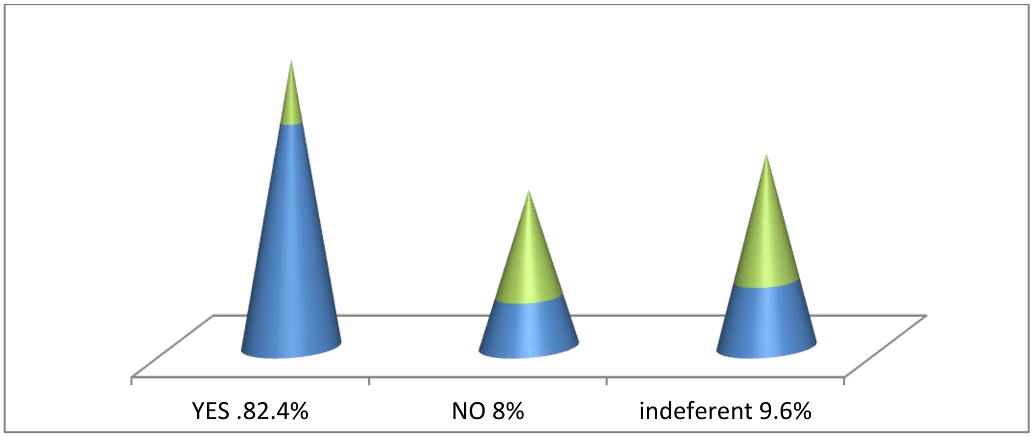

Figure 3: Impact of Cybercrime on Benin Youth

The above figure 3 chart brings to the understandingofhow Benin youths and the company they work for as stated in the serial number 12 on the Table 2 are finding it difficult with internet. A platform meant to improve lives of the end users has become nightmare, leaving them with no chance to get the best out of it and has become a huge effect in their ICT endeavour

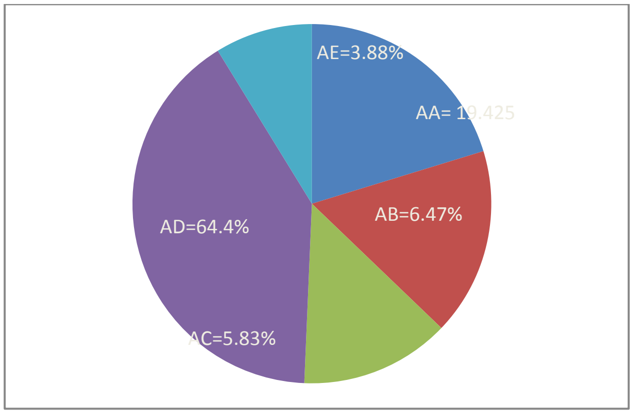

Figure 4: Impact of various attacks on Benin youth

5.0 Conclusion and Recommendations

Cyberspace has inherent features that enable users gain access to data. This allows intruders navigate through internet on a daily basis. There is no special key strong enough for protecting system, what an intruder needs is time to break the codes. This illicit act has continued to play a negative role in the daily usage of PC in Benin. There is no solid law or right protecting them from falling victim to this crime. From the analysis, it was observedthat 97.1% out of the 100%data sampled data affectedrevealed there were no legal action takenagainst these criminalsin demanding justice due to diversity of cultures, traditions and religious believe etc. We strongly believed that this is closed to the truth becauseAfrica as a continent is still growing. We therefore recommend the following:

1. Edo State government in collaborations with federal government should start educating youth on the methodology of this new crime currentlygiving the nation bad image: This can be done by integrating cybercrime as a course into tertiary institution curriculum as a general course for all 300 level to give all more knowledge on it
2. The punishments for cybercrime in Nigeria constitution be reviewed and replaced with a well enacted law.
3. Following the lack of boundaries in cyberspace the United Nations (UN) should create a formidable cybercrime laws replicated in all Countries and States withagency on cybercrimes fully empowered to punish any criminal found wantingand so as to remove the inactive cyber laws in some States. The issue on diversity in Religious beliefs, Culture,Traditions and Treaties amongst Countries will be isolated totally

6.0 References

[1] Michael Chukwujindu Ogwezzy. Cyber Crime and the Proliferation of Yahoo Addicts in Nigeria, Faculty of Law, Department of Public International Law,Lead City University, Lagos-Ibadan Expressway, Toll Gate Area, P.O Box 30678 Secretariat, Ibadan, Oyo State, Nigeria Email: ogwezzym@yahoo.com AGORA International Journal of Juridical Sciences, www.juridicaljournal.univagora.ro ISSN 1843-570X, E-ISSN 2067-7677, No.1 (2012), pp. 86-102 86

[2] N.A. Azeez, O. Osunade, Towards ameliorating cybercrime and Cybersecurity (IJCSIS) International Journal of Computer Science and Information Security, Vol. 3, No. 1, 2009

[3] MaitanmiOlusola,Ogunlere Samson,Ayinde Semiu,AdekunleYinka. Impact of Cyber Crimes on Nigerian Economy. The International Journal Of Engineering And Science (IJES) Volume 2 Issue 4 Pages 45-512013 ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805

[4] United Nations Office on Drugs and Crime (2013) February. Vienna Comprehensive Study on Cybercrime

[5] Tommie Singleton (2013), *The Top 5 Cybercrimes* CPA/CITP/CFF, Ph.D. Director of Consulting Services Carr Riggs & Ingram Enterprise, AL

[6] Schreiber, Sally P., “Dozens Indicted on Stolen Identity Tax Refund Fraud Charges,” Journal of Accountancy(online), Oct. 11, 2012. Last viewed Oct. 11, 2012, at journalofaccountancy.com

[7] Okonigene Robert Ehimen, Adekanle Bola (2009) cybercrime in Nigeria, Business Intelligence Journal

[8] Criminal Code Act-Tables - Nigeria Lawwww.nigeria-law.org/Criminal%2520Code%20Act-Tables.htmCriminal Code Act.Chapter77 Laws of the Federation of Nigeria 1990

[9] Cyber terrorism http://searchsecurity.techtarget.com/definition/cyberterrorism

[10] Difference between hackers and crackers - StudyMode.comwww.studymode.com › Home › Computers & Internet › Cyberculture