International Journal of Advanced Research and Development
ISSN: 2455-4030; Impact Factor: RJIF 5.24
Received: 22-06-2019; Accepted: 25-07-2019
www.advancedjournal.com
Volume 4; Issue 5; September 2019; Page No. 179-185

Cyber and computer related crimes in contemporary times: examining the causes, consequences and the preventive measures

Oriji Abraham[1], Young Denson Torunarigha[2]
[1] Department of Curriculum Studies & Educational Technology Faculty of Education, University of Port Harcourt, Nigeria
[2] Faculty of Education, Niger Delta University Wilberforce Island, Bayelsa State, Nigeria

Abstract
Technological advances have formed the basis for global economic growth, transforming of societies, especially our economies, and a substantial increase in standard of living, as can be observed in education, industries, government establishments, workplaces, and even at leisure (Ivanova, 2006). As the scholar further put it, "In many respects, the threat of cyber-attacks is escalating due to the increased availability of automated tools for malicious actions, the complexity of the technical environment, and the increased dependence of our society on interconnected systems. Therefore, protection of the information and communications infrastructures is vitally important." (p. 5). As a result, this paper aims to explain what Cybercrime is, and enumerate reasons for cybercrimes. It goes further to enumerate the consequences this criminal and/or illegal activities caused the society at large. Consequently, suggestions were also proffered on how to overcome the menace of this computer and cybercrimes in modern times.

Keywords: computer crime, computer fraud, internet crime, digital crime, and cybercrime

Introduction

The technological breakthrough experienced in the 21st Century has re-defamed and/or transformed our economies and societies, thereby forming the foundation for universal economic growth and subsequent increase in the standard of living. This transformation has been noticed in the industry, education, government and trade, workplaces, and in leisure (Iwanova, 2006) [19]. The advents of computers and the Internet respectively have enormously influenced almost all activities on the planet earth. This is the era of information and communication technology, where almost everything is digitized.

These technological breakthroughs have made life more meaningful as it has made an inroad into education, businesses, communities, and the lives of individuals (Chon, 2016) [9], changing the means that people interact, study, and work; making is easy for people in various parts of the world to communicate in real-time via a variety of devices, such as computers, cell phones, tablets, etc. It is no more surprising that text messages, emails, photos, videos that were formally shared by single individual could now be shared and viewed by hundreds or thousands of Internet or social media users in seconds or minutes (Hazelwood and Magnin, 2013) [18].

It is however highly regrettable as well that these technological devices, particularly the Internet technology that made life more meaningful (easy and less expensive) has also brought untold hardships to mankind as computer criminals have cost nations billions of naira and have put our personal and national security at risk (Bloombecker, 1990) [5]. In concord, Ivanova (2006) declared that criminals, terrorists, and wicked users, have exploited the anonymity and global reach of the Internet to use these technological devices that make lives more meaningful for us to launch attacks on the information infrastructure; put harmful and illegal content on the Internet; perform reconnaissance for physical attack; steal money, identities, and secrets; conduct hostile information operations.

In the same development, Chon (2016) [9] expressed the same surprise when the scholar stated thus "We rely on technology to make our lives more productive, and this occurs through the help of software. Unfortunately, software can also be used for disreputable reasons such as to steal data, disrupt and destroy systems, all of which have become more common in recent years." (P. 10).

Online criminals have emerged globally; it has become a new medium for all forms of misconduct, which ranges from threats, harassments, intimidations, etc. These illegal activities by cybercriminals have caused various harms to numerous Internet users. In affirmation to the above, Cross (2008) [10] said, "The ways in which criminals commit crimes are also changing. Universal digital accessibility opens new opportunities for the unscrupulous. Millions of dollars are lost by both businesses and consumers to computer-savvy criminals. Worse, computers and networks can be used to harass victims or set them up for violent attacks - even to coordinate and carry out terrorist activities that threaten us all" (P. 2).

From the onset of this century, there emerged social networking sites that provide platforms for individual, groups, companies, corporate organizations, to express their feelings, get new friends an connect old friends. Unfortunately, these cherished sites by individuals and groups have been misused by Internet criminals, popularly christened "cyber criminals", who want to accomplish their illegal purposes through the use of computers and other known technological devices.

The prevalent growths of these technological tools have led to new types of crimes and criminals observed today on the cyberspace. We are now in a new era where criminals

operate without weapons, where international criminals need no passports or visas to carry out their nefarious activities, a period where a number of bullets no longer count, and where computer keys are becoming more dangerous than the atomic bombs that aim to cause more mayhem than what happened in Hiroshima and Nagasaki (LeMay and Tibbets, 2014). This singular art has posed lots of challenges for the entire world, with the developing countries mostly affected. In fact, it is an ongoing threat that has become an issue of global concern.

Evans *et al.* (2010) [13] posit that these crooks adopt several means to achieve their objectives

- By responding to their bogus e-mails purportedly from your banks, and credit card company.
- Request of change of address for credit card bills
- Request of change of address for bank statements
- These crooks can open new credit card accounts in your name
- They can open new bank accounts in your name and write bad checks
- They can take out credits in your name and disappear with the proceeds, leaving you in debt
- They can counterfeit bank card and checks for your legitimate accounts, etc.

Let's examine some important concepts that may be invaluable for a better comprehension of the subject matter.

Stalking: Repeated harassing or threatening behaviour, in which an offender persistently contacts, follows, approaches, threatens or otherwise subjects a victim to unwelcome attentions.

Criminals: Classical philosophers, such as Beccaria (1764) [2] and Bentham (1891) [4], viewed criminals as actors that fundamentally chose to break the law on their own volition.

Cybercriminals: This refers to individuals who use computers, networks, and the Internet to perpetuate crime (Evans *et al*, 2006).

What is cybercrime?

Firstly, cybercrime is a combination of two words, that is, "Cyber" and "Crime." As a result, for better comprehension of the subject matter, let us examine some scholarly definitions or concepts of "Cyber" and "Crime." The Dictionary of Contemporary English (2009) [12] defined "Cyber" as a prefix relating to computers, especially to messages and information on the Internet. While Beal (n.d.), refers to it as a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers. The author further declared that anything related to the Intern*et* also falls under the cyber category. Invariably, cyber means computer network, computer, or virtual reality.

The Dictionary of Contemporary English (2009) [12] also defined crime as an illegal activity in general; illegal action, which can be punished by law, and something that someone is blamed for doing or criticized for doing. While chambers English dictionary defined it as, a violation of law, especially if serious; an act punishable by law; and an act gravely wrong morally. Generally, it means an abominable or immoral act that is punishable by law. Which means that any act that contravenes law and is subject to prosecution and punishment by the state is referred to as crime.

Consequently, "Cybercrime" is a very broad and all-encompassing term that covers a variety of activities that involves the use of computers (Cross, 2008) [10]. (Chang, 2012) [12] asserts that there is no agreed upon universal definition of what constitutes cybercrime. The scholar additional stressed that the terms, such as, "cybercrime", "computer crime", "computer-related crime", "hi-tech' crime", "technology-enabled crime", "online crime" "e-crime", and "cyberspace crime" are often used interchangeably. Again, jurisdictional dilemma has also been identified as another factor that makes a hard-and-fast definition of cybercrime extremely difficult. That is to say that laws in different jurisdictions define terms differently (https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html). In addition, a major problem for the study of cybercrime is the absence of a consistent current definition, even among those law enforcement agencies charged with tackling it (NOP/NHTCU, 2002) [21].

Thomas and Loader (2003) conceptualized cybercrime as those 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.' Cybercrime involves computers or computer networks, such as the Internet. In this case, computers and/or networks can be used to commit any crime, and could also be the target of any envisaged crime. Evans, Martin and Poatsy (2010) [13] defined cybercrime as any criminal action perpetuated primarily through the use of a computer. In the same development, Australian Criminal Code Act of 1995 describes cybercrime as "high tech crime" which includes:

- Computer intrusions (e.g., malicious hacking)
- Unauthorised modification of data, including destruction of data
- Denial-of-service (DoS) attacks
- Distributed denial of service (DDoS) attacks using botnets.
- Creation and distribution of malicious software (for example, viruses, worms, and Trojans)

Cybercrime vs Computer crime

As Cross (2008) [10] put it, cybercrime refers to criminal offenses committed using the Internet or another computer network as a component of the crime. However, there lies a little difference between cybercrime and computer crime. In this case, cybercrime is narrower than computer crime. Cybercrime involves any abnormal behaviour perpetuated through electronic operations via computer network/Internet that targets the security of computer systems and the data contained therein. While computer related crime may include all of the above, and in addition to those illegal acts committed offline with computers (Gercke, 2014) [16].

However, cybercrime is an umbrella term that involves activities, such as online child exploitation, state sponsored hacking and theft of hardware. Cybercrime is used to describe anything associated with computers, information technology, the internet and the diverse internet culture (Ratan (2014) [22]. These crimes are most times classified based on whether a computer is used as an instrument, target or merely incidental to a crime (Smith, Grabosky & Urbas, 2004) [27].

Ennin (2015) defined cybercrime as the means of using the ICT as a medium to defraud people.

Cross (2008) [10] in his attempt to define cybercrime

provided two definitions in both narrow and broader senses thus: cybercrime in a narrow sense is any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. While cybercrime in a broader sense is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

In totality therefore, any form of illegal act or crime committed, whereby a computer system or computer network, or similar technologies serve as the location, means, target or source of the act could be referred to as cybercrime.

Reasons advanced for cybercrimes in our society

There is an axiom which states that there is no smoke without fire. Yes, cybercrime has come to be, but it is quite pertinent to ask, "What actually are the reasons behind these fraudulent acts on the Internet?" What are the motivating factors for these cybercriminal acts? Many reasons have been advanced for these dishonest acts. Nonetheless, let's examine some of these reasons.

There is no doubt that cybercrimes are driven by a range of motivations. Based on the opinions of those concerned with combating hacking activities globally, there is a tendency to emphasize maliciousness, vandalism, and the desire to commit wanton destruction (Kovacich, 1999). While among the wider public, hackers are perceived to act on motivations ranging from self-assertion, curiosity, and thrill seeking, to greed and hooliganism (Dowland *et al*., 1999; Voiskounsky *et al*, 2000) [36]. From a 'rational choice' viewpoint, cybercrimes are deemed to be driven by a range of motivations 'as old as human society, including greed, lust, revenge and curiosity' (Grabosky and Smith, 2001) [17].

Chon (2016) [9] observed that in hackers' self-presentations as documented in some of their authored texts and documents as cited by Taylor (1999) [29] and Verton (2002) are motivated by factors, such as intellectual curiosity, the desire to expand the boundaries of knowledge, a commitment to the free flow and exchange of information, resistance to political authoritarianism and corporate domination, and the aim of improving computer security by exposing the laxity and ineptitude of those charged with safeguarding socially sensitive data (Evans *et al*, 2010; Vegh, 2002; and Woo *et al*, 2004) [13].

However, Taylor (1999) [29] skeptically notes that such self-attributed motivations may well be rhetorical devices mobilized by hackers to justify their law-breaking and defend themselves against accusations of criminality and deviance. The scholar further states that such accounts 'straight from the horse's mouth' do not necessarily furnish insights into hacker motivations that are any more objectively true than those attributed by outside observers.

Flores, Matsukawa, Remorin, and Sancho (2017) have advanced that strong political agenda might be one of the reasons why cybercriminals attack government organizations. As the scholars perceived, the motive of the crime could be to undermine the effectiveness of a government in order to reducing the faith of citizens in a particular government. This is in line with Taylor (1999) [29] and Verton (2002).

On motivation, Chantler (1995) recognized the sensation of thrill and excitement-seeking behaviour as a reason why offenders engage in hacking activities. Turgeman-Goldschmidt (2005) considered it as a type of social entertainment among a population of Israeli hackers. Hutchings (2013) identified monetary gain as a common spur for criminals when engaging in cybercrime.

Evans *et al* (2010) [13] have advanced other reasons that encourage cybercrimes. The scholars posit that some hackers like to snoop (spy or nose around). They break into systems for the sake of seeing what information they can find. Some hackers also break into systems for the challenge of it. These hackers, which refer to themselves as (White-hat hackers) do not intend to steal or cause any destruction. Some see themselves as experts that are performing needed services to the society or to corporate organizations to uncover the vulnerability of their systems in order to adequately protect them. These set of hackers look down on others who use their expertise to destroy information or do any other illegal activities. This group is referred to as Black-hat hackers (Evans *et al*, 2010) [13]. Regardless of the names given to them, the laws of the United States and many other countries consider unauthorized access to computer systems as a crime (Evans *et al*, 2010) [13].

The scholars posit that the reasons for cybercriminals (offenders) appear to vary. Again, it has also been implied that the social organisation and specialization of offenders has a role in offending behaviour (Broadhurst *et al*, 2013). The authors claim that the reason why an offender commits crime may also be a consequence of the people they interact with, that is, other offenders.

Types and consequences of computer and cybercrimes on society

There is no doubt that various forms of computer and cybercrimes are committed on a daily basis, and these illegal acts are seriously affecting our society in different dimensions (private individuals, governments, corporate organizations, and other agencies), and have become an issue of great concern not only for computer and Internet users, but to the entire society.

With the rate at which cybercrimes are being perpetuated, there is no doubt that every Internet user is vulnerable to cyber-attacks. There have been reports of financial losses of millions of naira or dollars on a yearly basis as a result of cybercriminals operations on the net. These criminals use the computer as an accessory to a crime; as a weapon of crime, as well as a target of a crime (U.S. Department of Justice, 2003). Different ways of perfecting these acts abound, such as computer espionage (spying), unauthorized access to computers, damage to computer data or programs, computer sabotage, unauthorized interception of communications, "child sexual exploitation", "revenge porn, "bullying", "cyber-stalking, "harassment. Thus, there is need to examine some of the consequences of these crimes in modern times.

Theft of Computer Resources. As Furnell (2002) observed, when hackers gain access to your computer, they may use the resources of the hacked system for their own purposes by storing illegal or undesirable materials in the system. The author further stressed that a hacker from Sweden illegally accessed an American university's systems, and used them to store and distribute a massive array of pirated music (MP3) files.

Theft of Proprietary or Confidential Information: Hackers usually steal or copy confidential information from the

computer system. This may be software, business secrets, personal information about an organization's employees and customers, credit card details which can subsequently be used for fraudulent purposes. Theft of proprietary information is cited as the greatest source of financial losses by business and other organizations (CSI/FBI, 2003). Customers' credit card details have constantly been stolen as a result of hacking incidents; hackers were able to exploit banks' systems to arrange illegal electronic transfers of funds (Riem, 2001; Travis, 2001; and Wilding, 2003). It is also on record that a Russian hacker known only as 'Maxim' accessed the systems of an Internet retailer and stole details of some 300,000 credit cards (Yar, 2006). In another instance, a group of hackers from Russia electronically transfer over $10 million from the accounts of Citibank's US customers (Grabosky and Smith, 2001) [17].

Systems Sabotage, Alteration and Destruction: Most computer users have suffered loses, such as systems sabotage, alteration and destruction. For instance, Philipson (2001) cited a case where some disgruntled former employees have unleashed such destruction upon their erstwhile employers in revenge for having been dismissed (Denning, 1999). Many individuals, groups, and government institutions have suffered because systems content have been altered or erased by hackers 'as a prank, protest, or to flaunt their skills' (Denning, 1999).

Website Defacement and Spoofing: Website defacements are some of the prominent forms of hacker activities (Furnell, 2002). Cybercrimes directly attack target Internet Websites, deface and altered the contents, only to advertise their skills, or to express their ideologically and politically motivated forms of protest against governments, businesses (Denning, 1999; Furnell, 2002). As well, sites of companies that specialize in providing Internet security solutions are also victims of these cyber-attacks (Denning, 1999; Furnell, 2002 and Woo *et al* (2004)). Furthermore, Lilley (2002); and Vegh (2002) declared that US, Hong Kong, and Colombian governments, the CIA and the US military, the UK Labour and Conservative Parties, the New York Times, recorded cyber attacks. These hackers have the capability to create a 'spoof' or 'fake' websites to deceive and re-directed unsuspecting Internet users. The content of the accessed websites is sometimes replaced and offensive speeches, pornographic imagery, or accusations about the victim's supposedly unpleasant business or political practices are featured, and these acts have caused lots of embarrassments to the original owners of such websites.

In a nutshell, examples of computer crimes committed without authorization includes: -

1. Falsifying email source information
2. Improperly accessing a computer system, or network
3. Interfering with someone else's computer access or use
4. Introducing a virus or other contaminants into a computer system
5. Modifying, damaging, using, disclosing, copying, or taking programs or data
6. Stealing an information service from a provider
7. Using a computer in a scheme to defraud, and
8. Using encryption in aid of a crime.

Examples of cybercrimes

- Copyright Infringement
- Child Pornography
- Piracy
- Cyber extortion
- Identity Theft
- Phishing
- Carding
- Spasms
- Cyber terrorism (https://www.quora.com/What-is-the-difference-between-cyber-crime- and-computer-crime).

Cybercrimes and methods adopted

There are different types of cybercrimes that are seriously affecting our society today. These crimes are committed through various means on the Internet. Among these are committed among individuals, business enterprises, governments and the society at large.

Crime against individuals

Cyber Bullying: This specifically refers to bullying that takes place online, which is usually perfected via threatening text messages, emails, and instant messages that are constantly and annoyingly sent to individual cell phones and email accounts. These bullies may be carried out by relations, friends or classmates, online acquaintances, and even anonymous users. Normally, most of those persons that carry out these criminal acts usually know their victims. Some cybercriminals hack and block users email accounts.

Exploitation of Children: Most times, innocent children are bombarded with pornographic materials. This they do by tricking them into revealing personal or embarrassing information and sending same to others. Some are told to send them some vital information.

Blocking of Email Accounts: These criminals sometimes exclude someone from an instant messenger buddy list or blocking their email for no specific reason

Hacking: Hacking is a method by which a person breaks into somebody's computer in order to steal some sensitive information, or hacks into somebody's email or instant message account and use it to send nasty or factitious messages while posing as the owner of the account. Most times, the owners of these computers may not be aware of the intrusion of their computers from a remote location with different types of software.

Creating Websites: Some of these criminals create websites to make fun of other persons, who may be a teacher, friend or fellow classmates

Cyber Stalking: This is a kind of online harassment wherein victims are subjected to a bombardment of online messages and emails.

Data Stealing: Cybercriminals usually target and hack individuals' data/information, such as credit cards, bank account numbers and other vitals are constantly being targeted and hacked for their nefarious gains. They impersonate and gain access to institutions' information/data, such as the banks. They oftentimes inform and convince bank customers that there is one problem or the other with their account details, and request them to give vital information to rectify such problems. Such victims will willingly give such information believing that the request is coming from the right source. These criminals also steal individuals' photographs from networking sites, especially Facebook to create fake accounts to dupe unsuspecting persons online.

Cyber Defamation: This is a slander conducted through any form of digital media, which is usually committed through

the Internet or any other technological devices. This is committed when libelous claims about an individual(s) are posted on a website or sent through an email (https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/what-is-cyber-crime.html). This act is very common in our society (Nigeria) hereby somebody is accused of what he/she never thought of, and posed on any of the social networking sites.

Cyber Stalking: This method is yet another form of cybercrime. This involves online harassment of persons through constant bombardment of online messages and emails. In a nutshell, they victims' lives more miserable. It also refers to a situation whereby cybercriminals monitor individuals' minutes per minutes online actions or activities. It is an unwanted or repeated surveillance in an attempt to harass and intimidates their victims. Cybercriminals use the Internet to locate unsuspecting or innocent individuals, engage same in conversations and convince and oftentimes invite such persons for personal social outings or meetings. This act oftentimes turns out to rape, especially when it involves women.

Child Pornography: Child pornography is another heinous crime that is daily committed by these cybercriminals. It involves certain activities relating to material involving the sexually explicit depictions and sexual exploitation of minors. This ranges from producing, distributing, and possessing any pornographic materials that portray a minor (somebody under the age of 18). Cybercriminals use the internet to obtain and share pornographic images and videos involving minors. It also involves the selling or buying of children. Various social networking sites have been used by these cybercriminals to perpetuate these illegal acts.

Murder & thefts: In the same development, some cyber perpetrators commit more serious crimes against their victims, such as thefts, and at worst, murder. Some thefts occur when these criminals violate copyrights and download music, movies, games and other software at will. Also, some malicious Internet-based software are used to steal data or causing damage to software present in the system.

Cyber bullying/Harassment: Online harassment or cyber bullying is a pretty common occurrence on such services. Other forms are cyber threats, obscenity, terrorism, human and drug trafficking.

Cyber Crime against people: This includes a wide variety of offenses. Criminals will hide behind fake promotions, offers, giveaways, etc, while giving you the illusion of security to get you to give up your personal information. Impersonating institutions, such as banks, they gain access to your information by convincing you that there's a problem with your account details and thereby ask you to 'rectify' it. Schemes, such as the Nigerian letter scam or the chain-letter scams that were once practiced via snail mail have now gone digital. Internet auction fraud is another way of duping people with non-delivery of product or misuse of credit card information.

Crime against businesses

A famous bank robber, Willie Sutton, was asked, "Why do you rob banks?" In response to the question, he was quoted as saying, "That's where the money is" (Cross, 2008) [10]. These criminals have taking the Internet as quick access of getting where the money is. As Cross (2008) [10] further put it, "It also makes sense that criminals are showing up in greater numbers online, because increasingly, that's where the money is." Cybercriminals have resulted to electronic businesses - e-commerce, online banking, and related technologies to dupe individuals and organizations millions of dollars of financial transactions taking place across network connections. Internet has become gateway of duping people with non-delivery of product and/or misuse of credit card information (Cross, 2008) [10].

Company systems are constantly being hacked by Cyber perpetrators as most business enterprises store their most vital information on servers. Flores *et al* (2017) declared that "They can choose to destroy or leak them, or where money is concerned transfer funds from an organization to someone else's account." The adverse effect of this act is that the customers of these business enterprises will lose faith in the organization, and subsequently the businesses can lose a significant number of their customers, thereby operating at a loss. At the same time, the resources that will be put to hire IT experts to avoid the future occurrence of such dishonest act(s) could have been channeled to more productive purposes (Flores *et al*, 2017).

Cybercrime against governments

As **c**ybercriminals are no respecters of persons, group/bodies, so also do they disrespect government organizations. These criminals or terrorists hack secure database of government agencies with the intention to misuse sensitive information and cause any form of disharmony in the aforesaid governments (Flores *et al*, 2017).

Overcoming the cybercrimes menace in society

The advent of the Internet in the 21st Century has brought the entire world closer and making is a smaller place for individuals to live. On the same note, this technology that unites us has also created a universal problem (cybercrime) that has continued to evolve, with new threats sprouting on daily basis, which technically needs urgent attention. As a result, in any sphere that is prone to crime, the individual(s) within the area will certainly guard against such criminality. Consequently, everybody using the internet/network should, as a matter of necessity exercise some fundamental precautions to avoid destructive nature of this devilish art. Hence, several measures have to be put in place to guard against the range (variety) of cybercrimes that are constantly committed day after day. In fact, the ways and the manners we hear of these crimes being committed today may stop some of us from using the internet.

However, Evans *et al* (2010) [13] posit that no foolproof protection method exists, but basic measures or precautions need to be put in place to guard against any private and other forms of information preserved on our computer systems. Consequently, major preventive measures have been suggested hereunder.

Software and Hardware: Tightly packed security devices that use a unified system of software and hardware should be used to protect any sensitive information that is uploaded or downloaded via the Internet. As well, popular antiviral software like McAfee, Norton, among others that constantly protect against the threats of cybercrimes and prevent customers from cybercriminals should be employed. Internet users are also advised to, at all time browse the internet behind a firewall and anti-virus switched on (https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/what-is-cyber-crime.html). Firewalls are software or

hardware devices designed to keep computers safe from hackers; they are used to close open logical ports to invaders and potentially make computers invisible to other computers on the Internet (Evans *et al*, 2010) [13]. Computer users should be armed with anti-virus package updates in order to update and guard their operating systems and web browsers.

Password: A well formulated long and complex alphanumeric passwords could be a very good antidote to cybercrimes. Passwords should be changed continually and carefully in order to beat the nefarious activities of cybercriminals. Keep good record of password changes and protect them so as not to be misplaced. Sensitive information/data, such as personal financial transactions in computers must be rightly guarded to avoid being accessed by hackers. However, Evans *et al* (2010) [13] have advised that as we create hard-to-guess passwords, that we should avoid using obvious passwords, such as first, last name and date of births.

Identity Theft: Presently, identity theft is very widespread on the Internet. Identity theft however, refers to when somebody illegally obtains your private information/data, particularly for economic reasons/gains. Someone may dishonesty or trickily receive useful information online from close friends/relatives through Whatsapp or Facebook with the aim of using it for mischievous acts. Therefore, it is very advisable to be cautious of personal and private information you give out on the Internet, especially the date of births, pet names and/or mother's maiden names.

In the same development, you need to help protect your children and wards against identity theft by being careful when sharing your children/wards personal information, and as well keeping an eye on the type of information they give out on the Internet or social media sites.

Children Internet Education: Parents should teach their children and wards about the most acceptable use of the Internet. They should be thought to report to them about all kinds of cybercrimes, such as online bullying, harassment, stalking, etc.

Security Alert: Knowing what to do when your identity had been stolen by cybercriminals is very important. A victim of a cybercrime, no matter where it took place is required to alert the law enforcement agencies, especially the police and any other appropriate authorities to start immediate investigations, and stop further crime. If the crime is committed in the bank, such crime(s) should be reported to the appropriate bank where the incident occurred. You could also place fraud alerts and get your instant credit reports.

Unsolicited Email: Computer users are warned not to open suspicious emails that are not with clear identity (not trusted), especially email attachments. Cybercriminals' don't only aim to steal information/data from systems to carry out their nefarious activates, but also bent on damaging the entire computer systems with the least opportunity.

Online conversations: Internet users, particularly social media favourites are warned to desist from engaging on online conversations with total strangers.

Photocopiers are Dangerous: Evans *et al.* (2010) [13] have warned users that photocopiers present potential dangers for identity theft. This is on the ground that most of the photocopiers manufactured in recent times contain hard drives that are capable of storing scanned information on them. Therefore, a hacker may get vital information from any of such public photocopiers. It becomes necessary to inquire from the photocopier's security measures in place before making copies from the machines.

Locking of Rooms: Hackers directly or indirectly gain access to computers at homes. Hackers directly sit at home and install hacking software in computer systems. Although, this act really occurs in homes, but necessary measures, such as locking the room(s) that contain computers, especially when strangers are around, and putting passwords to prevent unauthorized access to your computer(s). It is also advised to remove some vital components of the systems to prevent access. Indirect accesses to computers usually occur via the Internet. Once your computers are connected to the Internet, they are vulnerable to hackers because other Internet users can also access your system once connected. Hence, strong and up-to-date antiviral software is highly recommended to prevent hackers. The Use of malware sometimes refers to crimeware has also been a good measure to curtail the activities of cybercriminals (Chnag, 2002).

Anti-hacking laws: Different countries should be able to pass anti-hacking laws and vigorously enforcement such laws in order to curb cybercrimes. Some developed worlds should also partnership with developed countries to help prevent cyber terrorism (Chon. 2016) [9].

Cybercrimes acts should be reported to appropriate/relevant crime prevention authorities whenever dictated to avoid further havocs.

Cybercrime is against humanity, and should be every person's concern in order to keep yourselves and families safe from their immoral activities.

Summary

The 21st Century technological breakthrough that made life more meaningful has as well turned against us in various ways. These technological advances have become a new medium for committing several crimes via computers cum the Internet, as they are used for all forms of misconduct, threatening, harassing, intimidation and cause harm to computer and Internet users. Cybercrime has become the order of the day that affects individuals, corporate organization and governments at large. However, this paper discussed some concepts with regards to cyber/computer crimes. Major reasons advanced for the criminal acts, methods used, and consequently the consequences suffered by individuals, business enterprises, organizations and governments were concisely addressed. Finally, preventive measures were suggested to avert or combat the menace of cybercriminals in our society.

References

1 Beal V. Cyber. Retrieved from. 2019. https://www.webopedia.com/TERM/C/ cyber.html
2 Beccaria C. On crimes and punishments. *In* Chon, K. H. (2016). Cybercrime precursors, 1764.
3 towards a model of offender resources: A thesis submitted for the degree of Doctor of Philosophy of the Australian National University
4 Bentham J. A fragment on government. New jersey: The Lawbook Exchange, Ltd, 1891.
5 Bloombecker B. Specter computer crimes: What they are not and how they cost Americans business half a billion Dollars a year! Illinois: Business One Irwin, 1990.
6 Brandenberg D. Examples of cybercrime. Retrieved 20

January, 2019, 2018, from https://
7 legalbeagle.com/6307677-examples-cyber-crime.html
8 Chang YC. Cybercrime in the greater China region: Regulatory responses and crime prevention across the Taiwan Strait. Edward Elgar Publishing, 2012.
9 Chon KH. Cybercrime precursors: towards a model of offender resources: A thesis. submitted for the degree of doctor of philosophy of the Australian National University, 2016.
10 Cross M. Scene of the cybercrime (2nd Ed.). Massachusetts: Syngress. Cybercrime - effects and prevention. Retrieved 12 November, 2018 from, 2008, https://targetstudy.com/articles/cyber-crime-effects-and-prevention.html
11 Denning D. Information warfare and security. New York: Addison-Wesley, 1999.
12 Dictionary of contemporary English, England: Pearson Education Ltd, 2009.
13 Evans A, Martin K, Poatsy MA. Introductory technology in action, 6th ed. Pearson Education: new Jersey, 2010.
14 Flores R, Matsukawa B, Remorin LA, Sancho D. Cybercrime in West Africa: poised for an underground market. Retrieved 12 December, 2018 from, 2017. https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf
15 Furnell S. Cybercrime: Vandalizing the information Society. London: Addison-Wesley, 2002.
16 Gercke M. Understanding cybercrime: phenomena, challenges and legal response. Switzerland: ITU Publication, 2014.
17 Grabosky P, Smith R. Telecommunication fraud in the digital age: The convergence of technologies', in D. Wall (ed.), Crime and the internet. London: Routledge, 2001.
18 Hazelwood SD, Koon-Magnin S. Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. International Journal of Cyber Criminology. 2013; 7(2):155. Retrieved 18 January, 2019 from http://www.cybercrimejournal.Com /hazelwoodkoonmagninijcc2013vol7issue2.pdf
19 Iwanova P. Cybercrime and cybersecurity. Information and security: An International Journal, 2006, 18.
20 Lilley P. Hacked, attacked and abused: Digital crime exposed. London: Kogan Page. Mercer, E. (n.d.). Causes of cybercrime. Retrieved 27 https://itstillworks.com/different-types-cyber-crime-1981.html
21 NOP/NHTCU (2002). Hi-tech crime: The impact on UK business. London: NHTCU.
22 Ratan J. Cyber laws & information technology. India: Bharat Law House Pvt. Ltd, 2014.
23 Savanova P. Information and security: Cybercrime and cybersecurity: An international Journal, 2006, 18.
24 Schwarz C. Davidson G. Kelly MJ, Mc Gauran. Chambers English dictionary (7th ed.). Cambridge: Clays Ltd, 1988.
25 Smith R, Grabosky P, Urbas G. Cyber criminals on trial. Criminal Justice Matters. 2004; 58(1):22-23.
26 Taylor P. Hackers: Crime in the Digital Sublime. London: Routledg Verton, D. (2002) The hacker diaries: Confessions of teenage hackers. Berkeley, 1999. McGraw-Hill/Osborne.
27 US. Department of Justice (USDOJ), 2003, 11. Indicted in Interstate Theft and Fencing Ring That Sold $2 Million in Stolen Merchandise Via eBay Internet Auctions. Retrieved 20 November, 2018 from http://www.usdoj.gov/USBO/ilo/pr/2003/pr/12003_2.pdf
28 Vegh S. Hacktivists or cyberterrorists? The changing media discourse on hacking, 2002.
29 First Monday, 7, 10, October. Retrieved 17 November, 2018 from http://firstmonday.org/ issues/issue7_10/ vegh/index.html
30 Voiskounsky A, Babeva J, Smyslova O. 'Attitudes towards computer hacking in Russia', in D. Thomas and B. Loader (eds), Cybercrime: Law enforcement, security and surveillance in the information age. London: Routledge. What is cyber-crime? Retrieved 20 January, 2019 from https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/what-is-cyber-crime.html
31 What is the difference between cyber-crime and computer crime? Retrieved 3 June, 2019 from https://www.quora.com/What-is-the-difference-between-cyber-crime-and-computer-crime
32 Woo H, Kim Y, Dominisk J. Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology.* 2004; 6:63-82.
33 Yar M. Cybercrime and society. London: Sage Publications, 2006.