MISUSE OF MODERN TECHNOLOGIES FOR CYBERCRIME BY YOUTHS: THE UNIVERSITY OF BENIN EXPERIENCE

BY

ThankGod Onyebuchi, IBE
PG/EDU1306318

DEPARTMENT OF EDUCATIONAL FOUNDATIONS
FACULTY OF EDUCATION
UNIVERSITY OF BENIN
BENIN CITY

DECEMBER, 2019

MISUSE OF MODERN TECHNOLOGIES FOR CYBERCRIME BY YOUTHS: THE UNIVERSITY OF BENIN EXPERIENCE

BY

ThankGod Onyebuchi, IBE
PG/EDU1306318

A PROJECT WRITTEN IN THE DEPARTMENT OF EDUCATIOAL FOUNDATIONS, FACULTY OF EDUCATION AND SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER DEGREE IN SOCIOLOGY OF EDUCATION OF THE UNIVERSITY OF BENIN, BENIN CITY, NIGERIA.

DECEMBER, 2019

CERTIFICATION

We the undersigned, certify that this study was carried out by ThankGod Onyebuchi, IBE in the Department of Educational Foundations, Faculty of Education, University of Benin, Benin City, Nigeria.

_____	_____
PROF. C.N. MUSA	**DR. E.O. OSAGIOBARE**
(Supervisor)	(Head of Department)
Date:_____	Date:_____

DEDICATION

This study is dedicated to the Holy Spirit, my source of inspiration, wisdom, knowledge and understanding, on whose wings I soared though this programme and to my beloved mother Mrs. Lois Chineyeoku IBE (Late). Though you are not physically present, I am however happy today to have accomplished your wish and desire for me, sleep on mama.

ACKNOWLEDGEMENTS

The researcher wishes to express his unending gratitude to the Almighty God for His grace, mercies and love on him always. The researcher is most grateful to his supervisor and lecturer Prof. C.N. Musa for his untiring, relentless and prompt scholarly remarks, constructive criticisms, contributions and encouragement without which this work would not have been completed in time. The researcher is forever grateful to Dr. E.O. Osagiobare, Head of Department, Educational Foundations, Faculty of Education, University of Benin whose friendly and scholarly advice and encouragement added value to the study and the completion of the programme.

The researcher is equally indebted to Dr. Ike Aghaosa, Mr. E. Osawaru, Dr. Elvis Agbonlahor, Mr. Vincent Ebohon, Dr. S. Bode for their objective and scholarly contributions at various level of the study. The researcher is specially indebted to his lecturers in the Faculty of Education and other faculties, especially Professors I. Owie, K.O. Adeyemi, Mrs. C.N. Omoifo, (Barr) V.O. Ibadin who taught him Research and Statistics. Others include Professors K. Omoyibo, O.B. Osadolor and Dr. I. Nyonrere.

Sincere thanks go to the researchers' mentors Rev. and Evang. Mrs. Paul ThankGod Ekeasi, District Superintendent, Edo District/Executive Committee Member South-South Zone 5, Assemblies of God, Nigeria, for their parental backup during the study, Rev. Barr. And Dr. Mrs. G.O. Chime, Assistant District Superintendent, Edo District, Assemblies of God Nigeria, Amb. and Mrs. F. Nwabuko of Presco Nigeria Plc., Barr. & Dr. Mrs. G. Otokhila, Deacon and Mrs. Armstrong Obozokhae, Deacon and Mrs. Bolarinwa Johnson, Engr. Dr. & Mrs. G. Eghobamien, Mrs. O. Asemota, Mr. & Mrs. V. Airefetalor, Mrs. A.R. Arhelobhegbe, Mrs. H. Dim, Mr. & Mrs. V. Ilumah, Mr. & Mrs. E. Agberemon, Mrs. E. Agbon-Ojeme, and others too numerous to mention for their moral, financial and spiritual assistance and support.

He also appreciates his colleagues and course mate, Mrs. E. Obozokhae, Pastor P. Imoukhuede, Miss Hope O. Okeremeta, Mrs. Alomore, O. Omare, Mr. Afam S. Odionye, Miss Ogbe T. Patricia, Mr. Abiodun E. Arinju, Rev. F. Osasere, Mr. Lawal S. Sesan, Miss Omoruyi Jennifer, Miss Tariah C. Ibiso, Revd Fr. Emmanuel Ezuluofor, Olatude E. Omoyajowo and Mr. Chikelue F. and Chinyeaka for their friendly and lovely disposition during the programme and study.

The researcher's appreciation also goes to the Department of Academic Planning, Student Affairs Division, University of Benin, as well as students of the sampled faculties in the University of Benin for their cooperation and willingness to respond when contacted.

He sincerely appreciates his lovely wife Mrs. Blessing Ngozi IBE and children Liveth, Lifted, Treasure, Triumphant and Rejoice for their care, patience and understanding during the study. Finally, all those whose names are not mentioned here are more appreciated.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

This study was carried out to investigate cybercrime and the misuse of modern technologies by youths in the University of Benin. Cybercrime is vastly growing in the world of technology today. Cybercriminals exploit internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services and even gain access to classified government information. Many nations of the world have blacklisted Nigerian youths in connection with fraudulent and illegal internet activities and as such would not want to do any form of legitimate business transaction(s) with them especially on the internet with the fear of being scammed or duped. Cybercrime in Nigeria seems to be perpetuated by youths especially those in Universities and to a very large extent cybercrime seems to affect their educational pursuit and academic performance. The youths are of a great concern and importance to every society, so, whatever it takes, their development should be looked into so as to promote the goals of education. Nine research questions were raised and six hypotheses were formulated to guide the study.

The descriptive survey research design was adopted for the study. The population of the study comprised 43,772 students made up of 39,243 undergraduates and 4,529 postgraduates. The data was collected using simple random sampling technique and a sample size of 408 students was selected from the University of Benin. The research instrument used for the

study was a self-structured questionnaire. The instrument was subjected to scrutiny and test-retest reliability of 0.96 was derived, indicating that the instrument was reliable. The data were analyzed using frequency, percentage, mean, standard deviation, chi-square and t-test of independent samples statistics. The results revealed that unemployment, greed for money, poverty and parental conflict are among the leading causes of misuse of modern technology for cybercrime. Cybercrime activities can impact negatively on youths in the areas of academics, interpersonal relationships, social behaviour, and so on. Non-prosecution of cybercriminals by government and law enforcement agents encourages youths' participation in cybercrime activities. Peer influence encourage youths' involvement in cybercrime activities. There is a direct link between knowledge of internet and cybercrime activities. There exists a relationship between socio-economic status of youths and their involvement in cybercrime. Males are more inclined to cybercrime and deviant behaviours than their female counterparts. family and parents' socio-economic background is linked to youth involvement in cybercrimes and there is a relationship between education and cybercrime activities among youths.

It was concluded that the causative factors of youths' involvement in cybercrime can be curbed or reduced to its barest minimum and youths can be encouraged to uphold societal values and shun criminal tendencies. It was

recommended that the government should formulate workable policies against cybercrimes.

CHAPTER ONE

INTRODUCTION

Background to the Study

Cybercrime is a term used broadly to describe criminal activity in which computer networks are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories. Computer crime has been defined as `any illegal act facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime' (Royal Canadian Mounted Police, 2010). Cybercrime in all its facets is one of the fastest growing areas of criminality in recent times. More and more criminals are exploring the speed, convenience and anonymity that modern technologies offer to commit different crimes, including hacking into computer data and systems, impersonation, the distribution of child sexual abuse images and Internet auction fraud. The global nature of the Internet allows criminals to execute almost any illegal activity anywhere in the world, which makes it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace.

Other terms for cybercrime are “computer crime”, “computer-related crime”, “high-tech crime” and “Internet fraud” which are often used interchangeably. Crimes committed primarily through Internet contact include: credit card fraud, identity theft, child pornography, indecent chat-room behaviour, money transfer, spurious on-line datings, inciting propaganda, scandals. software piracy and network security breaches (Royal Canadian Mounted Police, 2010).

Easy access to modern technologies has resulted in many socio-cultural changes especially among young people. Technology changes the way youths interact and communicate with each other, which easily influences their way of life. Youths of different skills, backgrounds and educational levels develop different capacities dealing with technology in a new world. Indeed, modern technology has brought both positive and negative sides to our societies (Baker & Bidin, 2014).

While the positive sides of modern technologies could be the motives in obtaining and facilitating such technologies to youth, past studies have warned the negative sides of modern technologies could be harmful to one’s social behaviour. Longe, et al (2018) claim that a majority of youths are involved in various cybercrimes including e-mail scam, cyber bullying and intimidations, lying, website hacking, Internet pornography, child and drug

trafficking, pranksters, piracy, examination fraud, financial fraud and sabotaging Internet network providers. Igbo, Egbe-okpenge & Awopetu (2013) point out that although modern technologies advance education, economy and society, cautions must be taken when providing and investigating in such technologies, both at individuals and the national levels. They emphasize that parents, school guidance, counsellors and professionals outside the school need to play their roles in directing and protecting youths against the negative consequences of modern technologies that may cause problem to the society.

The easy access to modern technologies influences the behaviour of youths due to the absorption of foreign culture and behaviour that are incompatible with the nature of our societies, hence creating a gap between youths and their communities. Criminal behaviour includes involvement in cybercrime activities. To that extent, many researchers such as Baturay & Toker (2015), Passey et al (2014), al-Zahrani (2015), Mareschal, et al (2017) are calling for efficient and strict legal actions against youths found guilty practising and involving in such demeaning activities. Other researchers, practitioners and policymakers call for the imposition of concrete and efficient mechanisms to control the use of modern technologies to reduce

their negative effects on youths (Jonsson et al, 2014; Blinka & Smahel, 2006; Cupta & Parvesh, 2014).

Evidently, the misuse of modern technologies may bring unbearable consequences to society particularly the youths. Although the misuse of modern technologies among Malaysian youths shows an increasing trend (The Star Online, 2014), there is no significant effort that investigate this phenomenon. To the best of knowledge, there are no empirical investigated of the possible dangers of (cybercrime on Nigerian youths. The available case studies on Nigeria investigate the positive impacts of technology on youths. Yusop & Sumari (2016) examine the role of technology in assisting students in achieving their academic goals. They find that students are actively engaged in social media sites for information sharing and educational purposes.

Cybercrime is a global phenomenon and so is not exclusive to Nigeria. Akano (2013) maintained that cybercrime does not respect geographical boundary. Fighting the menace therefore can only be achieved through partnership with other cyber security organizations and institutions across the world. Cybercrime differs from most terrestrial crimes in four ways: they are easy to learn how to commit, they require a few resources relative to the potential damages caused, they can be committed in a jurisdiction without

being physically present in it and fourthly, they are often not clearly illegal. According to Director of Computer Crime Research Centre (CCRC) (2004) "cybercrime" is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. In essence, cybercrime is crime committed in a virtual space and a virtual space is fashioned in a way that information about persons, objects, facts, events, phenomena or processes are represented in mathematical, symbol or any other way and transferred through local and global network.

Cybercrime has surpassed illicit drug trade as global top revenue earner for organised crimes. The cybercrime network has become a highly organised ecosystem with its own value chain including: researchers of stronger attack methods; hackers who compress account data and make them available to dump vendors (Lemo, 2013). According to him, the industrialisation of cyber fraud poses a great challenge to the cash-less society in Nigeria. He said the prevalence of fraud globally is contributing to the growing technophobia (fear of using the Internet or modern technology) as users were apprehensive of the safety of their funds on electronic payment platforms. Crime remains pervasive and forever strives to hide itself in the

face of development. As measures and techniques for detecting crimes and criminals advance, criminals also look for means of evading them.

Nigeria loses over N127bn annually to cybercrime (Ewepu, 2016). The federal government has said that the estimate annual cost of cybercrime to Nigeria is 0.08 percent of the country's Gross Domestic Products (GDP), which represents about N127 billion. The Director-General, National Information Technology Development Agency (NITDA), Isa Pantami (2015), revealed that Nigeria suffered about 2,175 cyber-attacks in 2015. Pantami, who disclosed this at the inauguration of a committee to implement the National Cyber Security Strategy (NCSS) in Abuja, said a total of 585 government-owned websites were going among the 2,175 Nigeria websites hacked in 2015.

According to him, about 14 percent of the 97 million Internet users in Nigeria suffered cyber-attacks, which he said had necessitated the setting up of a Cyber Security Committee. Indeed, over the past 20 years, immoral cyberspace users have continued to use the Internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary recently, calling for quick response in fast tracking the implementation of Cybercrime Act,

which was passed into law in May 2015, and is expected to protect the cyber space and its users. According to him, Nigeria is the 56th out of 60 countries embracing Internet usage but third in the fraud attempt category. "We are tempted to ask why there is such an upsurge of e-crime in Nigeria and what are the factors that make Nigerians so vulnerable to e-crime?" (Peter Oluka, 2017:7)).

At the National Cyber Security Awareness Month Event organised by the American Embassy in Lagos, last year, Chairman, Cyber Security Experts Association of Nigeria (CSEAN), Remi Afon, while lamenting the negative impact of the menace on the country, called for concerted efforts in crushing its growing influence. In Nigeria, there has been increase in online presence, as there are currently close to 97 million Nigerian Internet users, according to the Nigerian Communications Commission (NCC).

According to the Executive Vice Chairman of NCC, Prof. Umar Danbatta (2016), there is a tendency for cybercrimes to increase, if nothing concrete is done to curb the trend, as the country begins 4G-LTE revolution with unhindered access to the Internet. He explained that "the expected explosion in high-speed Internet access also meant both those who use the Internet for legitimate and illegitimate businesses will now have increased access to the Internet". Noting that "all around the globe, we have seen

individuals, companies and governments become the victims of cyber-attacks". The US Consul General in Nigeria, John Bray (2014) said that cyber awareness is everyone's responsibility, calling on everyone to "join in cyber security awareness efforts across the country".

Akinsehinde (2011) argued that, over 80 percent of businesses with online presence in Nigeria are susceptible to cyber-attacks and the increasing spate of cyber-criminal activities was threatening the Nigeria economy. He argued that web portals and web-based applications of the Central Bank of Nigeria, Nigeria Stock Exchange, banks, pension fund administrators and switching/electronic payment companies had been found to be vulnerable to cyber-attacks due to inadequate security measures for safeguarding the platforms. Nigeria is also rated among one of the most corrupt countries of the world.

The contribution of the Internet to the development of the nation has been marred by the evolution of new waves of crimes. The internet has also become an environment where the most lucrative and safest crime thrives. Cybercrime has become a global threat from Europe to America, Africa to Asia. Cybercrime has come as a strange phenomenon in Nigeria. With each passing day, there are more alarming cases of cybercrimes in Nigeria, with each new case more shocking than the one before. Unfortunately, the

country's image has also suffered as a result of the unscripted activities of some Nigerians using the internet as a channel for the perpetration of criminal spamming activities. The major implication and challenge of the involvement in this menace in the Nigerian society in the nearest future there will be a high level of disinterest in education and touting among young people.

In Nigeria today, young people who engage in this form of anti-social behaviour for the purpose of living a life of splendour. Overtime, Nigeria has been labelled as a corrupt nation. There is the need for the Nigeria government to do something urgent to curb this menace of cybercrime. Diverse researches have concentrated efforts on the establishment of linkages among the human environment, increasing nature of technological driven business transactions, the growth of fraud and the attendant skepticism revolving around the security of online interaction globally. In one of such studies, Kovacich (2018) reveals that trade on a global scale has been increasing for centuries, and it is expected to continue to increase, in some areas expanding exponentially and more rapidly than in the past.

Kovacich (2011) predicted that between 2001 and 2006, $1 trillion worth of goods and services worldwide would be purchased online or influenced by information found about product and services. This projected

figure appears enormous and its realisation is expected to be facilitated by the Internet thus invariably raising a concern about the volume of financial burden and risk disposable factors inherent in e-business arena. Similarly, when one considers the mode and magnitude of online payment and the current dimension of acquiring goods and services globally, it is very clear that most nations will be forced to glue to the Internet or at best online trading in the foreseeable future. The realisation of this prediction places nations at a vintage point of risks. In the US, for instance, trading often takes place mainly in the form of credit and debit cards, while in Europe, Asia and Africa payment and reception of goods and services take place through bank or money transfers and cash delivery (Montague, 2011).

Quantifying the implications of these forms of payment as relating to transactions worldwide, cyber fraud business may as well enjoy more days of operations if adequate measures are not taken to arrest its tide. Most people and even most researchers believe that frauds is on the increase both in size and frequency which is difficult to know (Dutton & Helsper, 2009). Information on the magnitude of fraud often come from four sources: governments, researches, insurance companies and fraud victims (Albrecht et al, 2012).

Also, Fischer (2017), a German Foreign Minister, estimated that cybercrime cost Germany well over $40 billion a year. The magnitude of losses attributable to cyber fraud is worrisome. Apart from the monetary losses to nations of the world, cyber fraud has other social consequences, which researches should establish and document. This will include its cost to the criminal justice system with its potential of draining taxpayer's money and the cost of fraud needed to replace stolen/damaged property occasioned by such crime. There is also the need to evaluate the costs of fraud to the victim which entails reduced productivity, health expenses and socio-psychological shock.

Just as the international business is growing along with fraud activities, there is an attendant growth in the population of net fraudsters. It then becomes a challenge for governments, organizations and private individuals to take far-reaching steps that will neutralize the risks associated with online fraud. Therefore, this work on cyber fraud is divided into four sub-sections. The first examines cyber fraud, the second attempts the theoretical explanation of youth involvement in fraud in Nigeria while the third critically looks at the evolution of cyber fraud and finally, the fourth discusses the general nature of cyber fraud, and youths participation and closely followed by measures to be taken to arrest the tide.

It was reported that credit card and access device frauds are most common globally because criminals take advantage of their simplicity, acceptability and the variety of devices and information they contain for consumers in the world of business. The major driver of these fraud types remains the Internet which cyber fraudsters use to commit a variety of cybercrime. Shade & Shepherd (2013), and Tsukayama (2013) call for effective strategies that promote "digital policy literacy", to be directed to youth to help them understand communication policy process, the political economy of media, and the technological infrastructure of media institutions. Such policies may contribute to a more effective youth development and empower youth with the digital economy.

Statement of the Problem

In recent times, the Internet has experienced an explosive growth in different nations of the world. As the Internet grows to become more accessible with more individual becoming more reliant on it for their daily operations, so does the threat and hazards associated with it.

The impact of technology in modern life is unmeasurable, we use technology in different ways on a daily basis to accomplish specific tasks or the interest but sometimes, the way various technological appliances are manipulated do more damage than good.

Cybercrime is vastly growing in the world of technology today. Criminals of the world wide web exploit Internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services and even gain access to classified government information.

Many nations of the world have blacklisted Nigerians especially the youths in relation to fraudulent and illegal internet activities and as such would not want to do any form of legitimate transaction with them especially on the internet with the fear of being scammed or duped. Cybercrime in Nigeria appeared to be perpetuated by youths especially those in tertiary institutions and to a very large extent cybercrime seems to affect their educational pursuit and academic performance. The youth is of a great concern and importance to every society, so whatever their development should be looked into so as to promote goals of education.

Regrettably, cybercrime has equally engulfed the university communities as a replication of what obtains in the larger Nigerian society. Some students in universities and other tertiary institutions freely indulge in all sort of cybercrime activities with relative impunity. This has continued to create unimaginable challenges in the growth and development of the environment, and the educational pursuit of the youth's themselves.

One therefore, wonders whether any serious attention is being paid to curbing cybercrime among youths in Nigerian universities especially University of Benin. It is against this background that this study attempts to investigate the causes and effects of youth incessant participation in crime especially those implicated on internet use. It also explains youth condition and affiliation with crime activism within the social and economic environment, it formally suggest strategies needed to curtail their proneness to cybercrime.

Research Questions

The following research questions have been formulated to guide the study.

1. What are the causes of the misuse of modern technologies for cybercrime by youths in Nigeria?
2. What is the effect of the misuse of modern technologies for cybercrime on individuals and the society?
3. Does non-prosecution of cybercriminals by government and law enforcement agents encourage youths' participation in cybercrime in Nigeria?
4. Is there any significant relationship between peer group influence and youths' involvement in cybercrime in Nigeria?

5. Is there any relation between the knowledge of the Internet and cybercrime among youths in Nigeria?
6. Is there any relationship between the socio-economic status of Nigerian youths and their involvement in cybercrime?
7. Is there any significant difference in gender and youths' participation in cybercrime in Nigeria?
8. Is there any relationship between family and parents socio-economic background and youths' involvement in cybercrime?
9. Is there any relationship between education and cybercrime among youths in Nigeria?

Hypotheses

Question 1 – 3 were answered while 4-9 were turn into hypotheses and tested at 0.05 alpha level.

1. There is no significant relationship between peer group influence and youths' involvement in cybercrime in Nigeria.
2. There is no significant relationship between the knowledge of the internet and youths' involvement in cybercrime.
3. There is no significant relationship between youth socio-economic status and their involvement in cybercrime in Nigeria.
4. There is no significant difference in gender and youths' participation in cybercrime in Nigeria.

5. There is no relationship between parents' socio-economic status and youth involvement in cybercrime in Nigeria.
6. There is no relationship between education and cybercrime among youths in Nigeria.

Purpose of the Study

The study seeks to investigate the prevalence of cybercrime and misuse of modern technologies by University of Benin students. The specific objective of this study is:

- to ascertain the reasons cybercrime is gaining much acceptance among Nigerians especially the youths;
- to determine the factors necessitating the involvement of Nigerian youth in cybercrime activities;
- to identify the sociological and educational implications of the menace to individuals and the society;
- to establish whether gender influences involvement in cybercrime activities among youths in Nigeria;
- to determine the extent to which peer group influences cybercrime activities among youths in Nigeria;
- to show whether parents or family socio-economic status influences cybercrime activities among Nigeria youths;
- to ascertain the relationship between the socio-economic status of Nigerian youths and their involvements in higher crime;
- to suggest measures that can be taken by the government and society to curb cybercrime in Nigeria.

Significance of the Study

The study which is primarily aimed at explaining the misuse of modern technologies for cybercrime by youths especially in the University of Benin.

The report would be of great benefits to youths to expose them to the basic factors that tend to encourage young people into cybercrime activities in Nigeria by providing insight into the problem associated with the misuse of modern technologies for cybercrime.

It will be useful to the family and the recipient and sufferer of these criminal activities on how to encourage individuals especially the youths to uphold societal values and shun criminal activities.

It will also be useful to the government and stakeholders to adequately understand the basic factors responsible for and how to curb the continue spread of cybercrime and misuse of modern technologies by youth and the general public.

The findings will be useful for researchers to further generate knowledge in this field of study.

In addition, the findings will help the government to formulate workable rules and regulations against cybercrime and the misuse of modern technology among Nigerian youths.

Scope and Delimitation of the Study

This study is primarily focused on the issue of cyber and the misuse of modern technologies by youths in Nigeria.

Since university students are mainly youths, the study will be delimited to full-time undergraduate and postgraduate students of the University of Benin to investigate the causes, implication and provide possible solutions to the menace of cybercrime.

Definition of Terms

Cyber: Cyber is a prefix used in a growing number of terms to describe new things that being made possible by the spread of computers. Anything related to the internet also falls under the cyber category.

Cybercrime: Cybercrime is any crime that takes place primarily online through the use of computers. The computer may be used in the commission of a crime or the target.

Misuse: The act of using something in an illegal improper, and unfair way or misapplication of instrument to achieve a purpose.

Modern Technology: Is simply an advancement or improvement of old technological appliances.

Youth: A youth is a young person who has not reached adulthood. It is a period of life in between childhood and adulthood the age range of youth ranges from one society to another.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

This chapter presents a review of related literature on the misuse of modern technology for cybercrime by youths and the Nigerian experience. The review is done under the following sub-headings:

- Theoretical Framework
- Origin of Modern Criminology
- General Theory of Crime
- Concept of Cybercrime
- Cybercrime and Related Criminology Theorist
- Causes of Cybercrime among Youths in Nigeria
- Effect of Cybercrime among Youths in Nigeria
- Motivations of Cybercrime and the Misuse of Modern Technologies by Youths in Nigeria
- Peer Group Influence and Cybercrime activities among Youths
- Socio-economic Influence on the Misuse of Modern Technology for Cybercrime among Youths
- Education and Misuse of Modern Technologies for Cybercrime by Youths
- Role of Gender and Participation in Cybercrime Activities
- Cybercrime Activities among Youths in Nigeria

- Legislations on Cybercrime Activities in Nigeria
- Preventive Measures for Cybercrime and the Misuse of Modern Technologies by Nigerian Youths
- Summary of Reviewed Literature

Theoretical Framework

History shows that the relationship between crime and technology is not new. Although the hardware has changed across the span of time, the basic crime ideas remain the same. The significant change in modern times is on the increase in personal computing power as a globalised communication network. The networked technology has become more than simply a force multiplier, because not only the ideas about committing a crime are shared on a global scale, but these ideas are also put to practice across the global network at a very fast speed. Internet is a set of social practices; the kind of purpose to which we put the Internet that creates the possibility of criminal and deviant activities. The Internet provides the means to link up the many and diverse networks already in existence. Since commercialisation of the Internet during the mid 1990s, it has grown manifold. Even though the majority of worldwide total Internet connections are located in developed countries, these are however growing at a very fast rate in developing countries too. An unequal access also follows along existing lines of social exclusion within individual countries and factors such

as employment, income, education, ethnic disability are reflected in the patterns of Internet use (Castells, 2002). These inequalities point out the social characteristics behind the emergence of cybercrime and cybercriminals. Thomas and Loader, (2005) conceptualise 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. This definition reflects an important difference between crime (acts explicitly prohibited by law and hence illegal) and deviance (acts that breach informal social norms and rules, hence considered undesirable or objectionable). However, it is worthwhile that crime and deviance cannot always be strictly separated in criminology. The boundaries between the criminal and deviant are socially negotiated and have become a recurrent feature of contemporary developments around the Internet. Some criminologists argue that cybercrime is not a new type of crime but is same as non-virtual crime; it just uses new tools and techniques, while some others say that cybercrime is radically different and focuses on social structural features of the environment. Therefore, this study will hinge on social learning, differential association and space transition theories. The relevance of the theories to the study explains the common factors that influences the use of modern technologies for cybercrime by youths.

Social Learning Theory and Cybercrime

Tarde (1903) explains the fact that individuals learn deviant behaviour and it is not biologically inherent. Tarde observes that there are four main requirements in which social learning occur; first individuals must have a close contact with those they are imitating which can be family members, close friends or teachers; second, individuals must engage in imitation of their superiors; third, is that they must understand their behaviour i.e they need to know what the behaviour is like. The individual must be a role model to the person who is imitating the behaviour. This theory takes into account the fact that the behaviour learnt could be negative as well as positive. Another important contributor to this theory is Bandura (1977) who asserts that most human behaviour is learned observationally and this information serves as a guide for action in future. Through the process of socialization an individual learns the norms of society. An individual with less experience views the more experienced person as a mentor. For example, the act of hacking is learnt in group interaction. Even photo morphing is learnt for fun which can be later used for defamation. Most of the cybercrimes are learnt as they involve the use of technology.

Criminologists have also used two primary theories to explain and analyze cybercrime; Aker's (1998) social learning theory and Gottfredson

and Hirschi's (1990) generally theory of crime for example. Generally, theory is based on the premise that people with less self-control are impulsive, insensitive, short-sighted and risk takers, and are unable to resist the opportunity to offend. However, social learning theory proposes that crime is a learned behaviour stemming from peer association that leads to deviant attitude. Less self-control is also linked to various forms of cybercrime including illegal download of music, piracy of movies, software piracy.

Associating with deviant peers is one of these strongest correlates of crime and provides deviant models for imitation. "Social learning theory has significant intrinsic value for understanding cybercrime because offenders must learn not only how to operate a highly technical piece of equipment but also specific procedures, programming and techniques for using the computer illegally". Skinner and Fream (1927) many studies have found consistent evidence that associating with deviant peers leads to a wide variety of cyber deviance.

Differential Association and Cybercrime

This theory is most widely accepted theory in criminology. It was first proposed by Sutherland (1924) to explain the rise in white collar crimes. The basic idea behind this theory is that criminal tendencies are learned in

interaction with other deviant persons. It is through interaction with others that one engages in illegal acts. This theory could explain why normal law abiding individuals can turn into criminals or deviants, depending on the circumstances that they may be put into. This theory considers social environment as a means to explain why some individuals engage in criminal behaviour. This is seen in poor socio-economic conditions which encourage disobedience of law and authority. The main premise of this theory is that criminal behaviours is learnt through social interactions. The groups created on various social networking sites have framed their own norms and values for members. The new members have to accept these norms and values for online behaviour for close association. The norms of these groups often contradict with the norms of the society. Thus, through differential association with online deviants individuals are socialised into a subculture of deviance.

Space Transition Theory

"Space Transition Theory" is proposed by Jaishankar (2008). It explains the behaviour of the persons who bring out their conforming and non-conforming behaviour in the physical space and virtual space. Virtual space provides an individual with such space where he can express his feelings and even vent out his outrage against anyone. Cyber stalking and

Cyber defamation are instances where offenders use online space because of its anonymity and widespread approach. It also argues that people behave differently when they move from one space to another. One of the important postulates of the theory is that "People with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position'.

Origins of Modern Criminology

For much of Western history the dominant theory of the origin of crime was the "demonic perspective" (Einstadter and Henry, 1995; Pfohl, 1985). Crime was said to be the result of supernatural forces. People engaged in crime because they succumbed to the temptations of evil forces, such as Satan, or because they were possessed by evil forces. As Pfohl (1985) points out, this perspective can be summed up using the language of comedian Flip Wilson: "The devil made me do it". It also has a variant in Nigeria where people attribute everything good to God and everything evil to the devil. Nigerians often say `na devil work' or na as God want am'. Although no longer the dominant explanation of crime, this perspective can still be seen today. Many people, for example, argue that certain individuals engage in crime because they are "evil". According to the demonic

perspective, crime is sinful behaviour or an offense against God (or the gods). It is not surprising, then, that this perspective inspired very harsh reactions to crime. Brutal methods were often used to determine whether people were oppressed or had given in to evil forces, with many of these methods involving torture. Those found guilty were often brutally punished. For example, they might be burnt alive or otherwise slowly tortured to death in a public ceremony. These punishments were design "to purge the body of a sinner of traces of the devil and thereby restore the body of the community as a whole to its proper relation to God or the deities" (Pfohl, 1985:25).

The demonic perspective was dominant in the 1700s, but it was challenged during the Age of Enlightenment by a group of individuals who came to be known as the "classical" criminologists. Cesare Beccaria who was the first and most prominent of these criminologists published *An Essay on Crimes and Punishments,* in 1764 in Italy, which was immensely popular and had a profound impact on criminology and the Western legal system. The essential idea of "classical theory" was that individuals are rational beings who pursue their own interests, trying to maximise their pleasure and minimise their pain. And unless they are deterred by the threat of swift, certain and appropriately severe punishments, they may commit crimes

(harm others) in their pursuit of self-interest (Martin et al, 1990; Pfohl, 1985; Vold et al, 2002).

This theory differs from the demonic perspective in a fundamental way. Rather than argue that crime is caused by the supernatural or "other-worldly" forces, classical theory argues that crime is caused by natural forces or forces of this world – such as the absence of effective punishments. Supernatural forces cannot be observed, which means that the demonic perspective cannot be tested to determine whether it is true or false – there is no way to definitely test whether crime is caused by demonic possession. As such, the demonic perspective is not a scientific theory of crime. Classical theory focuses on natural forces that can be observed. For example, we can observe how swift and certain punishments are. As a consequence, we can test classical theory and thus it is seen as the first of the modern theories of crime. Classical theory dominated criminology from the late 1700s until the late 1800s. It then came under heavy attack, with Cesare Lombroso being one of its primary opponents. Lombroso's theory, first proposed in 1876, soon replaced the classical theory as the dominant explanation of crime. Drawing on Darwin's theory of evolution, Lombroso argued that many criminals are "genetic throwbacks", or primitive people in the midst of modern society. Their primitive, savage state is what leads them to engage in

crime. Criminals, then, are abnormal, irrational individuals who choose to engage in crime to maximize their pleasure and minimize their pain. They are fundamentally different from non-criminals, and these differences compel them to engage in crime.

Although Lombroso's theory differs from classical theory in some ways, it too argues that crime is caused by natural forces. Lombroso developed his theory after conducting extensive examination of criminals and non-criminals. He emphasized that theories must be based on or tested against observations of the world; in fact, he attacked the "armchair theorizing" of classical criminologists. Lombroso is sometimes called the "father" of modern criminology in part because of his emphasis on scientifically testing theories. It is important to examine the theories of Beccaria and Lombroso because of their enormous impact on contemporary theories of crime. Many modern theories of crime continue to argue that people are motivated to engage in crime through the pursuit of their self-interests and that what determines whether they engage in crime and the constraints they face, such as the threat of punishment.

General Theory of Crime

Traditional sociological theorists placed their primary focus on the social experiences of youths outside the family. For differential association theory for example, attention has been drawn to the role of peer groups in encouraging crime; while strain theory considered lack of opportunities in school and in the labour market as a source of crime – inducing frustration. In his social bond theory, Hirschi (1990:90) emphasized the importance of "indirect control," how close attachment of youths to parents allows them to have a "psychological presence" on them rather than when they are not under their watchful eyes or surveillance. In contrast Gottfredson and Hirschi (2006:98) have redirected the attention of criminologists to the family and to what parents do, or do not do during childhood.

Gottfredson and Hirschi (1990:90), however argues that "direct control" is the key to effective parenting (Wells and Ramkin, 1988). Unless parents and the society monitor their youths closely and take adequate steps to punish misbehaviour when it occurs and teach the youths that breaking rules has consequences, self-control will not be instilled. Instead, the youths "will tend to be impulsive, insensitive (as opposed to mental), risk-taking, short-sighted and nonverbal" (Gottfredson and Hirschi, 1990:90). As they endlessly succumb to life's temporary temptations, youths burdened with

low self-control will constantly engage in crime and other form of deviance. They also lack the persistence needed to succeed in school in the workplace and in social relationships. In short, they will be consigned to a wayward life replete with brushes with the law and with personal and social failure.

It should be noted that Gottfredson and Hirschi differentiate between "criminality" which is the propensity to offend a law. They recognize that a propensity cannot be acted on unless the opportunity. As a results they see crime as a by-product of people with low self-control, who have high criminogenic propensities, coming into contact with illegal opportunities. Still, given that most offenses are easy to commit and opportunities for crime are constantly available, over time people with low-self-control inevitably will become deeply involved in criminal behaviour. That is self-control not opportunities will be the primary determinant of people's involvement in crime across their life course. Similar to social bond theory, the core premise of Gottfredson and Hirschi, theory is easily identified and thus amenable to testing. The lower a person's self-control, the higher his or her involvement in criminal behaviour and in acts analogues to crime.

In general, there is a fairly consistent support for Gottfredson and Hirschi's theoretical predictions, a fact that ensures that their self-control theory, will remain an important theoretical perspective in the time ahead

(Gottfredson, 2006). The consistent support for the perspective is most apparent in Pratt and Cullen's (2000) meta-analysis of the existing of empirical research. They report that across studies testing Gottfredson and Hirschi. Theory of low self-control "had an effect size that exceed 20" a finding that would "rank self-control as one of the strongest known correlates of crime" (Pratt and Cullen, 2000: 951-952). The limits of self-control theory, however, should also be mentioned. Thus, in empirical test, low self-control cannot as Gottfredson and Hirschi predict, explain away the effects of other sociological factors on crime especially the effects of differential association/social learning. Perhaps more consequential, Gottfredson and Hirschi (1985:185) call it the "fallacy of autonomy. The belief that what goes on inside the family can usefully be separated from the forces that affect it from the outside.

Concept of Cybercrime

Theorists of the internet agree that cyberspace makes possible near and instant interactions between individuals who are spatially distant, which creates possibility for new forms of association which in turn gives rise to cybercrime and cyber deviance. Cybercrime, is a crime that is facilitated or committed using a computer, network or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. It can take place on the computer alone, or in other

virtual or non-virtual locations. It is recognised that current legal definitions of cybercrime vary drastically between jurisdictions. A practical definition of a cybercrime is offered by Kshetri (2010). According to him, "Cyber Crime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offence or violating law, rules or regulations". Examples of cybercrime include denial of service attacks, cyber-theft, cyber trespass, cyber obscenity, critical infrastructure attacks, online fraud, online money laundering, ID fraud, cyber terrorism, and cyber extortions. It is evident that organized criminal organisations use cybercrime extensively to collaborate and connect with their vast network which is spread across the globe. The synergy between organised crime and the Internet has thus increased the insecurity of the digital world.

Categories of Cybercrime

It is very important to identify the various categories of cybercrime and categorise them. Cybercrimes can be easily placed into two categories; violent and non-violent cybercrimes. Most of the cybercrimes are non-violent offences, interaction is without any physical contact. Some of the non-violent cybercrimes are cyber trespass, cyber theft and cyber fraud. The categories and types of cybercrime are presented below:

Cybercrimes

(a) Violent Cybercrimes

(i) Cyber Terrorism

(i) Cyber Theft

(ii) Cyber Stalking

(iii) Cyber Fraud

(iv) Pornography

(v) Cyber Trespass

(vi) Cyber Bullying

(vii) Fraud-Identify Theft

(viii) Drug Trafficking Deals

(ix) Malware

(x) Spam

(xi) Logic Bombs

(xii) Password sniffing

(xiii) Wire tapping/illegal Interception of tele-communication

(b) Non- Violent Cybercrimes

- Embezzlement
- Unlawful appropriation
- Corporate Espionage
- Plagiarism
- Piracy
- Identity Theft

(ii) Other Non-violent Cybercrimes

- Cyber Prostitution
- Online Gambling
- Online Trafficking
- Internet Drug Sales

(iii) Destructive Cybercrimes

- Cyber Vandalism
- Viruses

Fig. 1

Source: https://www.researchgate.net.

Violent Cybercrime

Violent cybercrimes pose a physical danger to some person or persons.

They are further classified as follows:

(1) *Cyber Terrorism*

A cyber terrorist can be described as someone who launches attack on government or organization in order to distort and or access stored information stored on the computer and their networks. According to Wikipedia, a cyber-terrorist is someone who intimidates a government to advance his or her political or social objectives by launching computer-based attack against computers, network and the information stored on them. For instance, a rumour on the Internet about terror acts. In addition, Parket (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 assessing and distorting any useful information in organizations or Government bodies using Computer and the Internet is generally referred to as Cyber Terrorism.

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. Cyber extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service.

(2) *Cyber Stalking*

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. People leave a lot of information about themselves online. Such information can leave one vulnerable to cyber stalking, a term that essentially refers to using the Internet to stalk (to illegally follow and watch somebody), Justin (2010). Whereas the content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interest parties (www.wikipedia.com).

(3) *Cyber Bullying*

Cyber bullying is an extension of physical bullying. It has two forms: overt and covert. Overt bullying is physical aggression and includes beating, kicking and sexual touching. Overt bullying is often accompanied by covert bullying in which victims are excluded from friends group, stalked, gossiped about, verbally harassed and threatened. Cyber bullying is carried by adolescents through the Internet. As more and more youths are using the Internet for interpersonal relationships, the risk of being bullied is increasing. It leads to depression, anger and sometimes even suicide.

(4) *Pornography*

Cyber pornography is the act of using cyber space to create, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber pornography is a criminal offense, classified as causing harm to persons.

(5) *Fraud-Identity Theft*

Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about that person. For instance, making a false bank webpage to retrieve information of account of an individual. The concept is simple; someone gains access to personal information and uses it for personal benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to Automatic Teller Machine (ATM) and using such people can make themselves a lot of money with personal information. 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.

(6) *Drug Trafficking Deals*

Another type of Cyber Crime is Drug 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

advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals at Internet cafes, use courier web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimated individuals to make comfortably purchase of illegal drugs (www.wikipedia.com).

(7) *Malware*

Malware refers to viruses, Trojans, worms and other software that access computers unnoticed. Back in the early part of the century, most of such software's primary aim was thrill. The people writing the software found it amusing to write a programme that exploited security flaws just to see how far it could spread. Today the incentive for making such software is generally more dangerous. In some cases a piece of malware will pretend to be a legitimate piece of software. 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.

(8) *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, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam. Some of these address harvesting approaches rely on users not reading the fine print to agreements, resulting in them agreeing to send messages indiscriminately to their contacts. This is a common approach in social networking spam such as that generated by the social networking site (Saul, 2007).

Spamming remains economically viable because advertisers have no operating cost beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer (Gyongyi, 2005).

(9) *Logic Bombs*

A typical logical bomb tells the computer to display certain instructions at a specified date and time or under certain conditions. The instructions may tell the computer to display “I spoil” on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in tandem with viruses. Whereas a simple virus infects a programme and then replicates when the programme starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular programme is run a certain number of times. Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn’t find the employee’s name, it crashes, destroying not only all of the employee payroll records, but the payroll application programme as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes.

(10) *Password Sniffing*

Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone system and network provides. Password sniffers are programmes that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user's name and a password-as required when using certain common Internet services like FTP (which is used to transfer files from one matching to another) or Telnet (which lets the user log in remotely to another machine) – the sniffer collects that information. Additional programmes sift through the collected information, pull out the important pieces (e.g, the user names and passwords), and cover up the existence of the sniffers in an automated way. Best estimates are that in 1994 as many as 100,000 sites were affected by sniffer attacks (David, et al, 1995).

(11) *Wiretapping/Illegal Interception Telecommunication*

There are several ways that physical methods can breach networks and communications, for instance, if telephone and network wiring is not protected both from intruders who can physically damage it and from wiretaps that can pick up the data flowing across the wires, criminals sometimes gain access to such communications

Non-Violent Cyber Crimes

Non-violent cybercrimes do not cause any physical damage to persons; instead they cause financial loss, psychological disorders and social harm. They are further classified as follows:

(i) *Cyber Theft*

Cyber theft is a way of using a computer and the Internet to steal money or information. This has been corrupted as “yahoo” in Nigeria, and hence `yahoo boys’. It is the most popular cybercrime in recent times because the ability to steal from a distance reduces the risk of detection and arrest. Cyber theft includes:

- *Cyber Embezzlement:* Cyber embezzlement means the misuse or alteration of data by an employee of a company who has legitimate access to the company’s computerized system and network. Example – an employee misusing the company’s computerized payroll system in such a way that he/she is paid extra.
- *Unlawful Appropriation:* Wherein an individual gains access from outside the organization to transfer funds and modify documents in such a manner that it gives him legitimate right to property he doesn’t own. Unlawful appropriation, differs from embezzlement as the offender is not interested in the valuables but in gaining access and transferring funds or modifying some information.
- *Corporate Espionage:* In this crime, an individual from inside/outside the company uses the network and steals marketing strategies, trade secrets, financial data, client lists etc in order to gain a competitive

advantage. In corporate or industrial espionage, the person uses the company's network to steal trade secrets, financial data, confidential client lists, marketing strategies or any other information to gain a competitive edge.

- *Plagiarism* is to steal someone else's original writing and call it one's own. This form of crime is increasing everywhere as more and more people have access to computers and the Internet.
- *Piracy* is an unauthorized copying of copyrighted software, video, music, books, etc which causes loss of revenue to the owner. Cyber piracy is the appropriation of new forms of intellectual property, in which the computer programme, expressed in the form of a digital code, generates through a computer system `virtual products' such as images, music, office aids or interactive experiences. When cyberspace and intellectual property laws interact they become a powerful force, especially in present day society where economic profit is quite important.
- *Identity Theft* – In this victim's personal information is stolen by the criminal to commit financial frauds.

(ii) *Cyber Fraud*

Another form of cybercrime which has a firm grip on society is cyber fraud and scams online. But, the problem with this is the lack of systematic and official data. Internet Crime Complaint Centre (ICCC) is the only source available whose primary role is to receive public reports of cybercrime and refer them to the relevant criminal justice agencies for action. A growing number of Internet action sites provide thieves in the global market the opportunity of selling stolen items to unsuspecting customers. Another form of reported fraud is non-delivery of items which the victims have already paid for. It can also include product in authenticity and misrepresentation of the condition of the item. In the cases of shill hiding, the seller places false bids by either using multiple fake identities or aliases to place bids on their own items or by arranging for associates to place bids for the items with no intention of actually purchasing them. Thereafter it becomes impossible for the legitimate bidders to detect whether or not others are genuine buyers or shills. In recent years, phishing and spoofing frauds have increased.

Phishing proceeds through the mass distribution of emails that purports to originate from banks, credit card companies and e-sellers. These mails request for providing personal and other details in order to update their account. The fraudsters thus gain access to the password and other security

and authentication information of users, which can then be used to hack bank accounts or steal through credit cards. According to the Anti-Phishing Working Group (APWG), there were over 2,500 such sites reported on the Internet in January 2005 alone, a 100% increase in the number in comparison to previous year (APWG, 2005). Phishing remains one of the most pernicious forms of cyber attack. The technical requirements are modest, no exotic zero-day vulnerabilities, no clever hacking techniques. And it leverages on one of the hardest weaknesses to fix in the technological environment. (APWG Q4 Report, 2018).

Cyber Trespass (Hacking): In the case of cyber trespass, a computer or network is accessed by the offender without authorisation, but may not misuse it. For example, a teenage hacker hacks a network just to prove himself to his peers or takes it as a challenge. These trespassers enjoy reading emails of others but they don't use any information they find. However, cyber trespass is a crime in majority of countries. Cybercrime causes more harm to society than traditional crimes. Hacking attack on World Trade Centre, Bhaba Atomic Research Centre, RBI are examples of cyber hacking, Hackers do so because of curiosity, a desire to learn, discover and to freely share what they discover about others, damaging those systems intentionally or otherwise.

- *Cyber Prostitution:* It involves carrying out prostitution online through various advertisements on sites, state.
- *Internet Gambling:* It denotes customers who use credit cards online to place bets in virtual casinos.
- *Internet Drug Sales:* Online pharmacies sale of drugs to customers who are unable to purchase it from public or private dealers. Most persons explore this medium to sale expired or fake drugs to their unsuspecting customer.
- *Cyber Laundering:* It means using the net to hide illegal money. Online banking offers opportunity to criminals who open accounts in an offshore bank and transfers funds electronically.

Destructive Cybercrime

In destructive cybercrimes, network services are disrupted or data is damaged or destroyed, rather than stolen or misused. They are classified as:

Cyber Vandalism: Is a form of vandalism that includes defacement of a website and denial of service attacks.

Spread of New Viruses: Many viruses are linked to notable dates, such as Christmas, Valentines Day or April Fool's day, as by doing so, virus writers and distributors feel that they have better chance of success. Some of the viruses (e.g CodeRed, MyDoom), unknown to their owners and/or users,

`infect' computers and are used to access personal information illegally. For example, they can be used to gain access to credit card numbers and then those numbers can be used to purchase goods and services illegally.

Cybercrime and Related Criminology Theorist

Several theories have explained why youths engage in crime and cybercrime. Some of the theories which range from classical to modern and post-modern period are explained briefly in this section.

Classical Sociological Theorists

Comte's (1865) positive philosophy is his real contribution to social and political philosophy. For him Positivism is the last stage of intellectual development. Reason and objectivity is the basis of positivism of his philosophy. Comte gave more importance to analysis, experimentation and observation. According to him, positivism is not only responsible, but inevitable for social reconstruction. It is essential for bringing a new society and new social order. Even though Comte did not talk about crime, but reason which is the basis of positivism has a strong foothold in conduction of crime. Many of the crimes are organised and planned reasonably so that least of the suspect is left behind. Criminals use their brains as much as intellectuals so that no footprints are left behind. They are objective and use reasoning and observation for criminal acts. Even cybercrime has a logical

basis as it involves analysis, objectivity, technical knowledge, experimentation and observation for criminal acts. Comte also believes that social development is the outcome of the development of human mind. As the human mind progresses, the society also develops and criminal tendencies and new types of crime emerge. Following the footsteps of Comte, many classical sociologists favoured the scientific approach to study society and social problems.

Durkheim (1893-1933) gave the notion of social solidarity and identified two major types: the Mechanical and the Organic. Mechanical solidarity means the integration that results from specialisation and interdependence. It is a consequence of moral and material density. Material density denotes a rise in population while moral density refers to the rise in interaction among people in society. The contemporary society has seen the emergence of organic solidarity of mechanical society. While mechanical society is dominated by respective laws, the organic society is predominated by restitutive laws. The type of society restores the status quo by using administrative machinery. New groups and interests develop and so do new criminals and crimes. Cybercrime is a feature of organic solidarity where heterogeneity complexity occurs. According to Durkhein, there is no society without crime but instead, every society has crime and is normal. In his view,

crime occurs when an individual diverges from the collective norms and exhibits a criminal character. Further, he views crime as a collective function which is important for reinforcing social norms and increasing consensus. Cybercrime is no doubt borderless and it occurs in abstraction, without any face-to-face interaction. It has brought together government of various countries on a common front to make laws to fight against cybercrimes.

Weber (1991) introduced `rationalisation' to explain societies in the west which have shifted from traditional orientation to rational and scientific orientation. Rationalisation is a process which replaces traditional and subjective thinking with reason and objectivity. He believed that history has seen societies with traditional mode of thinking and modern society has been rationalised. Even though rationalisation results in technological advancement, Weber feared that it would lead to dehumanized and alienated human. Rational society is based on social actions with "rationally pursued and calculated ends", where "the end, the means, and the secondary results are rationally taken into account and weighted". They involved an actor's calculation of the best means of achieving a given and (example how to make maximum profit by online theft) or even a consideration of different ends. Weber notes that the utility of each end is considered and there is a ranking of the utility associated with each end and, therefore, ends having

greater utility are pursued first in comparison to less important ends. All these features are suitably applicable for crime and cybercrime as well. Cybercrime can be committed by known as well as unknown persons. Cyber criminals know that it is easier for them to commit `e-fraud' in comparison to committing fraud in physical space. They have calculated ends and means. They commit crime in such a manner that leaves negligible chances to be caught.

Marx's (1932-1844) concept of alienation can be aptly used as a tool for understanding contemporary society. Technology has become a part and parcel of present society and Marx has referred to production as a technical process as it involves technology. Man has attempted to gain control over nature by means of technology. Great success is achieved and man has obtained large degrees of control over nature, time and distance. However, the control and order exercised by technology seem to extend over man himself. It appears human being have lost control over his own invention. The Internet designed to find solution to people's problems now poses issues difficult to control. It is the dynamics of technology because humans have engrossed themselves in this all powerful social fact. According to Marx, alienation renders people powerlessness. Indiscriminate use of modern technology has alienated human from themselves and people around them.

People have themselves become an objective or material in the organisation of modern technology leading to powerlessness; an aspect of new globalisation culture that has deprived people from face-to-face relations due to the process of globalization. Virtual world poses many challenges for the society. Even though many types of cybercrimes such as cyber bullying, cyber defamation and cyber blackmailing occur in virtual environment but they do have an effect in real life. However, it is very difficult to control these online crimes in physical world because of the lack of adequate knowledge and expertise which is required to deal with online crime. This causes alienation in present generation who although is techno savvy and active on various social networking sites feel powerless to deal with cybercrimes.

Pareto (1961) states clearly that every individual performs both logical and non-logical actions. In fact, everyone tries to justify even non-logical actions as logical. He also believes that every social phenomenon has two aspects: one is reality and the other is its form. Whereas the former involves the actual insistence of the thing, and form is the way in which phenomenon presents itself to human mind. The former he calls objective and the later as subjective aspect. He also believes that all actions of the individual have two aspects; one being the end and the other being means to

an end. When the means employed for achieving ends are correct, we call the action is logical otherwise they are non-logical. Similarly, in technology, many actions seen as logical by the actor (subjective) cannot be logical in reality (objective). For example, Hackers view hacking as useful and profitable. The viewers of porn sites never see it harmful. Nevertheless, cybercrime is a severe form of deviant behaviour but deviants justify it as logical and acceptable.

In view of Veblen (2003), the process of social change is more or less constant, and one change results in another change. Whole process of change cannot be resisted. For him social change indirectly reflects our technological advances and vice versa. The use of the Internet has established online communities which have brought new kind of social relationship. Relationships on networking sites also turn real when people are seriously involved. It is through the use of technology that people learn more about worldly affairs. Use of mobiles and the Internet for instant communication has become commonplace. However, technology has also given rise to a new type of crime i.e cybercrime. Online crime can be conducted from anywhere and at any time with a computer and a network connection. It leads to easy victimisation. Pornography has degraded social and moral values of youngsters and even children.

Tonnis (1991) mentions the concepts of Gemeinchaft and Gesselschaft. In Gemeinchaft (community) each person has some sort of relationship with others (without a choice), while in Gesselschaft (association) members enter into interaction according to their individual desires for achieving some specific purpose. Association has elements of self-interest whereas community has the element of co-operation and interdependence. The emerging world society falls in the category of Geselschaft where communication is virtual and individuals enter into relationship on their will for some specific motives. Such interactions occurs on social networking sites where individuals freely enter or leave a relation as per convenience. However, it has led to emergence of negative consequences such as cyber bullying, cyber defamation and cyber stalking.

Modern Sociological Theorists and Cybercrime

Merton (1938) opines that the gap between approved goals and the means creates strain. In contemporary society, success is primarily measured in terms of material achievements and social standing. In a mixed economy individuals have to choose their own path and work hard to earn a living. This leads to competitive nature of careers and employment. Merton used anomie theory to apply specifically to deviant behaviour in various societies. In the contemporary society, success is probably rated a lot higher than

virtue. His theory proposes that those individuals, who are underprivileged, may end up as taking honest and socially acceptable path to meet financial success and yet not end up as successful, as those who are not in the same position. This would lead them to question why they would take the honest path when they could be more successful through deviant behaviour. Cyber criminals come from diverse backgrounds. Those who are in higher schools or colleges are most likely to fit into these theories. They may see how they put a lot of hard work into their studies and development of skills and yet realise that it is unlikely that they could achieve the financial success. As a result they may see crime as a means to achieve enormous financial success. Any individual would see computer crime as a way and means to make large sums of illegitimate money.

Modernity recognises the advantages of technology and sees risk as its inevitable feature. The question is how can this risk be prevented, minimised or channeled. In classical modernity, the ideal was equality while in contemporary modernity, the ideal is safety.

Giddens (1991) describes the modern world as a `Juggenaut' which is a runaway engine of enormous power which, collectively as human beings, we can drive to some extent but which also threatens to rush out of control and which could render itself asunder. Internet is a product of modern

technology moving along time and over physical space. Digital citizens are the agents who steer it in their directions. Distanciation i.e close linkage between time and space is broken through the net. In this sense, both time and space are devoid of content and have become pure forms. Thus, with modernisation, time is standardised and the close linkage between time and space is disappearing. Relationship with those who are physically absent and increasingly distant are more and more likely. Time and space distanciation is important in modernity for several reasons; first it links local and global domain world, is able to mould the present, and third, such distanciation is a major prerequisite for the source of dynamism in modernity – i.e `Disembedding'. Disembedding involves lifting out of social relations from local levels of interaction. It has given rise to online relationships with those who are physically absent and increasingly distant. Social relations online are globalised and people do have friends from all over the world now. Friends are now made on the basis of common interests and goals. There are two types of disembedding mechanisms that play a key role in modern societies. First are symbolic tokens and second are expert systems. `Symbolic tokens' are money, which allows for time space distanciation. We are able to engage in transactions with others who are widely separated. This has also given spurt to online frauds and hacking through which cyber

criminals can make transactions from any part of the world at any time. The use of credit cards online exposes the user to the risk of identity misuse and eventual fraudulence. Second mechanism i.e `Expert System which involves professionals like lawyer, physicians and engineers; common things like cars, gadgets are also created and affected by Expert Systems. They provide guarantees (but not without risks) of performance across time and space. Personal Computers are always prone to viruses while using the Internet. Trust is very important in modern securities dominated by abstract systems. Online trust on someone with whom one is transacting or forming any relationship plays an important role but because of lack of physical proximity, it becomes easier for an individual to break the relationship at his own will and at any time because he or she is not answerable to anyone. Cyber experts are limited in number because of the technical skills required in this field which are complicated and difficult to learn. Besides this, cybercrime is conducted from any part of the globe at any time by anyone. Giddens talks about new and dangerous risks associated with modernity that always threatens our trust. Risk is global in intensity (cyber war). A wide range of public knows about the risks we face and are also aware that expert systems have a limited role to play.

Beck (1992) calls modern world a `Risk Society'. The emerging new modernity and new technologies are associated with the risk society. The contemporary world has elements of both. Beck labels the new or better yet newly emerging form as reflexive modernity. A process of individualization has taken place in the west. The agents of modern era are free of structural constraints and as a result better able to reflexively create not only themselves but also the societies in which they live. Beck recognized a strange paradox in late modern society; risk is increasing due to technology and science rather than being abated by technological progress. It is not a world which is less prone to risk, but it is "world risk society" as Beck explains. With the magnitude of risk so great, that transcends both time and place, by becoming global in scope, the control of risk `is both impossible and meaningless. In the case of cybercrime one is unaware of the risk that can occur with a single click of mouse. Hacking, fraud and online schemes are some of the risks to which users are exposed. The `Information Society' is thus creating risks for people thereby exhibiting a `Risk Society'. In the case of cyber risks, the weapons are software and knowledge, the environment in which the attack occurs is virtual; the possible attacker is unknown and is able to hide himself effectively.

Post Modern Sociological Theorists and Cybercrime

Post-modern society has seen the dawn of sentiments and emotions. In the modern era, the disadvantages of technology are recognised. While in modern society individualism was important, in postmodern era, emphasis is on collectivity or groups.

Baudrillard (1984:78) believes that there was a time when signs stood for something real, now they refer to little more than themselves. Distinction between what is real and what is fabricated is the cornerstone of the postmodern world. The distinction between signs and reality has imploded. It is characterised by such implosions as distinguished from explosions (of production system, of commodities, of technologies so on). Therefore, just as the modern world underwent the process of differentiation, the postmodern world can be seen as undergoing dedifferentiation, in a world where signs no longer have a natural meaning and are instead manufactured to take on symbolic meanings. According to Baudrillard (1984:78) `we live in the age of simulation'. It leads to "reproduction of objects or events". Software Piracy or the counterfeiting and distribution of products intended to pass for the original is done by illegal downloading. In photo morphing, a face can be morphed with someone else's body; it is difficult to distinguish real from the duplicate. Baudrillard describes the postmodern world as hyper reality. For example, stealing the IP address or identity of another computer

or to obtain access to the other computers on the network (Spoofing). Only a decade ago people had to trek down from one place to another for shopping. Now with a single click of mouse, these are available at one website from which we can order online. Shopping, banking, games, movies, entertainment, etc are available online. In rationalising these form of re-enchantment, they are by definition disenchanting them. Besides this, e-commerce has given rise to a number of online cybercrimes. Identity theft and online transactions are examples, in which fraud can be conducted without physical circumstances.

Janeson (1991) recognizes that postmodernism is usually associated with a radical break. He describes this new form as a `cultural dominant'. According to Jameson four elements are basic to postmodern society:

- Postmodern society is characterised by superficiality and depthlessness. It truly depicts the use of the Internet and its activities. Emergence of social networking sites coincide with superficiality as the people who are connected through these networks lack the basic connection and sentiments which are required for long lasting relations. Jameson has used the term "simulacrum" in which one cannot distinguish between original and the copied.

- In Postmodern society, emotions or intensities have faded. It causes alienation and anomie. Jameson prefers to call it as `Intensities'. The new electronic media gives rise to postmodern intensity. In cyberspace, humans lose their real self and dream about illusions in a virtual environment, which gives rise to unusual fantasies. Pornography is an example of such phenomenon.
- In Postmodern society, there is a loss of historicity (pastiche) i.e the past cannot be traced. All one has is the access to our texts or pictures. Even on the net one has to trust the information posted on it.
- Postmodern society has impressions based on reproductive technologies, especially electronic media like TV, computer, and the Internet. The postmodern era gives birth to new and varied cultural products than the explosive, expanding technologies of the modern era did. Cyber culture has produced a new type of culture in society which has both positive as well as negative aspects in it. For instance, infringement of copyrights (Plagiarism) has increased on the Internet.

Thus we realise that postmodernity is full of technical advancements but it carries within itself the forces of destruction. Cyber war is no exception to that. Developed and many developing countries rely on networks and servers

for important services and activities. Economic strength definitely depends on them. They ensure good society too.

Causes of Cybercrime among Youths in Nigeria

Materialistic Outlook: Today the simplicity of life is diminishing and it is being replaced with craving for materialism and consumerism. The children of the middle and affluent classed today have more money to spend than those of the past. Unmonitored spending by children could make them purchase things harmful to them.

Impact of Globalization: One of the consequences of globalisation is the influence of certain more permissive cultures on the so far traditional societies. For instance, the view that dating from an early age is an innocuous practice is influencing the adolescents and incidence in schools with young boys and girls getting emotionally and physically close are now common in Nigeria, fortunately in most cases, in normal friendly manners.

Increasing Loneliness of Children

This is another factor that is worth mentioning. With the breaking up of joint families and parents getting busier, children are left to themselves. With waning warmth and support of elders, children seek the company of peers and also find technology as surrogate parents and friends to overcome

loneliness, which affect interpersonal relationship and social behaviour among youths.

General Erosion of Values

In the society today, there is a general erosion of values and adults themselves often cease to be role models for the children. There are studies indicating that habits like smoking and drinking are due more to the influence of the adult members of the families than of peers. Licentious behaviours by adults influence children and they could emulate it at schools. Reliance on traditional norms that help us in differentiating between the good and evil is diminishing today in the technology driven world. In the past, extra marital sex and sex before marriage were considered as evil but today the taboo associated with such behaviours is diminishing as technology helps to prevent at least the physical damage that could be the fallout of such behaviours.

Easy Access to Unethical Values

Today it is much easier for the adolescents to procure things that are not meant for their age group. The technology facilitates access to films, videos, websites, etc, not meant for them. Similarly, magazines and books that could have an unhealthy impact on the adolescents are easily available in the market. Also, drugs, cigarettes, and even liquor are not very hard to

purchase. The rising incidence of drug addiction, substance abuse at parties, consumption of liquor by school children are a testimony to it. Incidence of children smoking in school campus is common. Laws and law enforcing agencies are cleverly dodged as the adolescents procure such things, thus exposing the limited utility of laws and policing in checking such procurement. However, it is through the right type of education that youth should be able to decide for themselves what has to be avoided.

Role of Technology

Today technology is accessible to a wide section of the population and most of the young learners of even developing countries have an access to it. The youth have an edge over the other age groups in adapting to new technologies and extracting their full benefit for various purposes. While technological devices have several utilities, including that for learning, yet they are also liable to be misused and in such cases can have adverse impact on individuals. Not only is access to unhealthy experiences made easier, but also, the individuals themselves are today in a position to create unhealthy content. For instance, there are photos of a woman almost naked online assaulted and battered by a man and his wife in Ibino, Ibom Local Government of Akwa Ibom State (Patrick Odey, Punch News August 17, 2019). Today, there are many children who are getting addicted to video games and there have been several incidents where excessive playing of video games led to serious consequences.

Influence of Media

There are several cross sectional as well as longitudinal studies to indicate that exposure to violence, aggression and other such negative experiences through the media can have adverse impact on young people. Even criminal behaviours like rape, abuse of spouse, homicides, etc, have

been linked to continuous exposure to such acts through the media during childhood. There are researches that support the general idea that impact of violent television programmes, films, video games, and even certain types of music enhance aggressiveness in the young people and have a negative impact on their personality. Exposure to unhealthy content can also enhance sexual urges. The media is playing an important role today in shaping the young culture. Incidents of campus violence as well as romance, dating from an early age, trying out addictive substances such as tobacco and alcohol are to a great extent behaviours that are the emulations of those dished out and even glamorised by the media.

Vulnerability of Adolescents

Adolescents are more vulnerable to perform certain activities. They exhibit heightened emotionality and also may suffer from emotional instability. Hormonal changes lead to new feelings and physical changes that make them desire the company and there is also a search for identity and the need for independence, which could make them rebel against the norms and practices of the society. Adolescents today try to experiment with addictive substances and indulge in sexual activities because of hormonal changes leading to heightened sexual desires coupled with thirst for unethical values.

The Internet as a Safe Place for Criminal Activities

The internet offers a valuable opportunity to fraudster to disguise themselves and their identifies. These fraudsters also change personal attributes such as age, gender, ethnic group, country of residence and so on. Even though the fraud is detected, identifying the culprit is very difficult. Victims of online frauds may be reluctant to report their victimisation due to the following reasons; relatively small amount of money involved does not make pursuing the matter worthwhile, embarrassment in reporting a fraud, ignorance about reporting the offence to the concerned authority, likelihood that no results will ensue as the fraudster is located in another country.

Reluctancy to Lodge Complaints about Cybercrime

Individuals and companies are reluctant to lodge complaint about cyber fraud. They remain silent on such issues to protect their reputation in international market in an era of liberalisation and globalisation. Not a day passes by that a cyber fraud is not perpetuated in our country. Its magnitude is increasing by leaps and bounds.

Quest for Wealth

Another cause of cybercrime in Nigeria is quest for wealth. There exists 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 cyber criminals require less investment and a conducive environment. Nigeria is such an environment and many cyber criminals take advantage.

Weak Implementation of Cybercrime Laws and Inadequate Equipped Law Agencies

Weak/fragile laws regarding cyber criminals exist in Nigeria. Other crimes and offence such as armed robbery are treated with maximum penalties. Unfortunately, the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals. Laura (2012) state that "African countries have been criticised for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime" Nigeria is not an exception to this rule. Furthermore, it is therefore paramount that the nation's legislation should ensure proper implementation of their laws against cybercrime.

Negative Role Models

Youths are mirrors of the society, but it's quite unfortunate how parents neglect their rightful duties. Meke (2012) remarked that today many parents transmit crime values to their wards, via socialisation as if it is values which ought to be transmitted to the younger generation. Imagine a

situation where the child supplies the father with vital information to wreck individual's banks account using the computer system, while the mother impersonates the account holder/owner at the bank. If this culture is imbibed among the younger generations most of them will see no wrong in cybercrime practices.

Effect of Cybercrime among Youths in Nigeria

Reduces the Competitive Edge of Organisation

The misuse of modern technology over the years have cost a lot of havoc to individuals, private and public business organisation within and outside the country, causing a lot of financial and physical damage. Such crimes may threaten a nation's security and financial health, a company can suffer losses due to computer crime when a hacker steals confidential information and future plans of the company. And he simply sells the information to a competitor company; this will automatically reduce the competitive strength of the company.

Time Wastage and Slow Financial Growth

Wastage of time is another problem because many IT personals may spend a lot of time on handling, rectifying harmful incidents which may be caused by computer criminals. The time spent should have earned a profit to the organisation. One peculiar problem is that, when a hacker enters an

organisation and steals confidential information from the company, the people who have trust in the company loses their confidence in the company as the company may contain confidential information like credit cards of customers and as the information is stolen, they will move to another company that they can entrust with their personal information.

Defamation of Image

With high level of cybercrime in the nation, the slogan "GOOD PEOPLE GREAT NATION" by Nigerians will be tarnished and the global community will see the country in a bad light. Other effects include the consumption of computer and network resources, and the cost in human time and attention of dismissing unwanted messages.

Effect of Cybercrime on Youths

Lack of Interest in Academics

The internet has become an essential part of the youths life and many of them are addicted to it and so become sleepless, giving less attention and time to their studies. Usually, they get involved in hacking and other criminal activities. ***Disconnection from Family Member***

Most parents do not have any idea of what their wards do on the internet, so the youths are fearless and are free in visiting and site without knowledge of the negative effect. The over use of the internet affects

psychological and mental relationship of youths, although they are connected to their peer groups, they are disconnected from their family living in the same roof. They constantly play online games on the Internet with little or no regard for outdoor activities, thereby destroying relationship between families and friends.

Affects on Physical and Mental Health

There are some sites which give lawless and unethical information which can destroy people's physical and mental health. Physically, they may have eyes, neck and muscular problems which can be life-long. The adult content that is given on the Internet causes immorality and negative thoughts in the mind of the youth which leads to stress, depression, and confusion – youths are today forgetting social values and norms, they become moody and nervous, many of them claiming that it is loneliness, depression or the hunger of seeking knowledge that spurs them into net surfing.

Motivations of Cybercrime and the Misuse of Modern Technologies by Youths in Nigeria

A motivation involved in cybercrime depends on criminal's intent and need. The following are the common motives behind cybercrimes:

1. ***Monetary Profit:*** Like many offline crimes, cybercrime are also motivated by the desire for financial gain.

2. ***Political Motive:*** The Internet is used by extremists and radical groups for propaganda, to attack the websites and networks of their opposite groups.
3. ***Sexual Impulses:*** Sexually deviant behaviour is illegal and is considered harmful. People view porn sites to fulfill their immoral desires and needs.
4. ***Entertainment:*** Many cybercrimes are done for fun and enjoyment unlike other cybercrimes, in which the Internet is a means to an end. For cyber criminals such as hackers, fun is both a means and an end.
5. ***Emotional Motivators:*** Cyber criminals who use anger as motivation are spurned lovers, fired employees, business associates or someone who feels cheated. Revenge is much better planned than anger and it could be more dangerous because cyber criminals have more time to think and plan their tracks which often reduces the possibility of being caught.

Peer Group Influence and Cybercrime Activities among Youths

Peer pressure has been linked to criminal behaviour, but it has not been found to be the primary reason why most youth engage in criminal behaviour. Peer pressure (or social pressure) is the direct influence on people

by their to changing their attitudes, values or behaviours to conform to those of the influencing group or individual.

According to Akers (1998) social theory, “individuals becomes deriant and maintain criminal tendencies through a dynamic social learning process hinging on differential associations. Individuals become exposed to crime and deviant definitions models and reinforcement based on their differences in association patterns”. Therefore, associating with deviant peers can be one of the strongest correlates of crime. Scholars have fouond consistent evidence that associating with deviant peers can change the behaviour of an individual (Akers and Lee, 1996).

Peer relation have long been central to the youths are particularly vulnerable to per dynamics study of crime and delinquency because they spend much time with them (peers) attribute great importance to them, become their primary role model and are more strongly influenced by them.

Thus, it is not surprising that one of the most consistent and robust findings in the criminology literature is that youths with criminal peers are more likely to participate in criminal behaviour. This finding which dates back to the 1930s with Shaw and Mckays (1942) discovery that more than 80% of juveniles appearing before court had peer accomplices (Tade and Aliyu, 2011).

In a study by Farrington (2002) opined that criminal offences reach its peak at adolescence or youth stage. This can be better explained by the impact that social influences have on this particular stage of life, especially by peers that seems to encourage unlawful behaviour. According to Haynie and Osgood (2005) at this stage, they spend a lot of time with friends and consider them very important which justifies the investment in research on the association between youth behaviour and peer group influence.

There is a strong association between youths participation in cybercrime and their peer group influence. That is, youths who have criminal friends are at more risk to develop criminal behaviour than those which without criminal friends (Hayne and Osgood, 2005).

It should also be considered that the association with deviant or criminal peers is normally done in two ways. Having friends who commit criminal act and join a more or less organized groups. The degree of involvement in cybercrime tend to be higher for teenagers and youths who claim to be members of a gang. Three major theoretical perspective explains this.

Individual characteristics that emphasizes the selection process, under which people with similar interests and behaviour tend to associate i.e similar ones attract each other.

Social learning, which emphasizes the process of socialization by the group, where a youth learns values attitudes and behaviours.

Interaction perspective which emphasizes the process of facilitating delinquent behaviour in which association with deviant peers plays a moderate role in aggravating the pre-existing problem of crime behaviour. Two way influence effects are more properly observed between youths behaviour and their peer influences (Baerreldt, Knecht, Raub, Snijiders and Steghch, 2010).

In all facts of human interaction, specific attitudes combine with social factors to produce behaviour. This is further reinforced by the subjective norms that are often driven by our beliefs about what others think we should do. In essence, social pressure to conform often lead individuals to behave in ways that are at variance with their inner convictions (Ajzen, 1991).

Consequently, in discussing youths' participation in cybercrime and peer influence, it must be viewed from the context of social psychological ideology underpinning human relationship and existence. Drawing from the influence of Jenkins (2008), modern times as a concept means modern concerns about identity, and modern processes of identification. The youth identification logo remains the internet technology. One of the theories that

best describes the current issue is the social impact theory which present a more unifying standard of social influenced. It states that the amount of influence others have in a given situation is a function of three factors which include: strength immediacy and number. Considering the impact that peer influence has on cybercrime participation as presented in these three variables therefore. Latane (1981) posits that social action of any kind and the total impact of others on a specific target, person or group of persons is a function of the interactors strength and that which is firmly derived from the status of the influence(s) involved on the one hand and their appealing abilities and the nature of relationship residing in the compelling power possessed by the influenced on the other hand.

Situationally, any given group become more influential for two obvious reasons, first, as influence builds up more people share their concern and second is when attempt is made by those external to appropriate the gains that can be derived from participation in the group. In this case as individual share in their concern of a group increases, the expected innovative response of entrant diminishes and the existing group becomes a reference point for present and future actions.

There is a spontaneous acceptance and imbibing of group practices. The defining characteristics binding the elements in the group together form

the basis for capability and association. In the fraud arena the bracketing in age, sex, taste, socio-economic conditions and host of other factors existing among the youths that are mostly involved in cybercrime often form the basis for association and closeness.

In addition, the social impact inherent in group morality often transferable from one element in the group to significant other simultaneously generates most observable similarity (Jegede, Olwookere and Elegbeleye, 2016).

Latane (1981) posited that "the existence of people characterized by like mindedness and bounding into clauster with the intention of realizing group goals help to provide answer to the emerging trend in crime participation among youth in contemporary times". According to Jegede et al (2016) in Latane (1981) peer influence constitutes the dynamic social impact propelling the youths to identifying with their counterparts in cybercrime environment. Youth within this reality forms a bound within which their aspirations are articulated, exercised reinforced and sustained in the atmosphere of similarly held attitudes, group values and the perception of their world (Francoi, 2003). The role of group influence on initiating and reinforcing both positive and negative behaviour has been widely reported

by different scholars for instance. Peer influence accounts for a significant portion of youth misbehavior (Kandel, 1973; Fraser and Kawkins, 1984).

Socio-Economic Influence on the Misuse of Modern Technologies for Cybercrime among Youths

Socio-economic status could be defined as individual position within a hierarchy of social structure based on occupation, education, income, wealth and place of residence.

Parents Socio-Economic Status and Youths Participation in Cybercrime

Parents socio-economic status can influence youths' participation in the misuse of modern technologies for cybercrime factors such as education and income are key factors that are predictive of youths maintaining a crime-free behaviour. This is because family socio-economic status can affect youth's perception of life which could lead to a change of behaviour.

Parents socio-economic status is a multidimensional concept of special importance for the growth devilment of behavioural patterns and education of youths. Since its definition generally refers to the amount of parents' income, employment status and lack of education. Hence lack of economic resources and low socio-economic status of parents may affect all aspect of the child's life as well as his or her social inclusion. Accordingly, the consequences of a reduced parental socio-economic status may leave long term effect on their children.

Though there are other factors that tends to influence youths' misuse of modern technologies for cybercrime, like peer group but parents socioeconomic background from all indications appears to be prevalent factor that encourages participation in the misuse of modern technology for cybercrime. The family especially the parents are the child's basic socializing agents. Maggie (1995) opines that a youths gain their first standard of behaviour from home. Imbosa (2002) adds that youth from poor socioeconomic background seek support and understanding elsewhere.

Youth Socio-Economic Status and their Participation in Cybercrime

Youths with personality problems arising from social conditions have been found to be involve in the misuse of modern technologies for cybercrime. The social and economic status of most Nigerians is below average, poverty and unemployment is on the increase, therefore youths roam the streets looking for a means which sometimes lure them to participate in cybercrime. Poverty tends to be a characteristics of social deviant behaviour including cybercrime. Poor economic conditions are worsened when the youth do not see any hope of employment even with education. It is therefore clear that socioeconomic background of youth may not be the driving force behind their participation in cybercrime.

Consequently, it can be said that, youth in cyber fraud business engage it, in part, as a result of prevalent norms among the economically battered group and in part to overcome the excruciating socio-economic circumstances in which they find themselves in Nigeria. The perception of belonging to the same socio-economic predicament and the experience of scuttled aspirations inform the borrowing of ideas from one another in an attempt to guarantee their survival within a society they have perceived as totally unfriendly.

The existence of strain caused by economic closure forms the basis for group identity and several resultant activities located in crime. The hopelessness generated by Nigeria's socio-economic climate of mass unemployment, deprivation, hunger, starvation and poverty affects the studied group's behavioural choice. Research has linked current social crisis to youth unemployment (Sesay, Ukeje, Aina and Odebiyi, 2003). Concomitantly, other research work also lamented the state of poverty in Nigeria (Ajayi, 2006; Ozughalu, 2008). Establishing affinity between poverty and crime, NISER report (2003) asserts that when poverty is coupled with high levels of economic and social aspirations, the stage is set for criminal activities particularly official corruption, robbery and dealing in illegal goods and services. It is incontestable that the medium of cyber space

creates an avenue for money both legally or otherwise under the social climate of poverty and mass unemployment mainly affecting the youths. It presents the opportunities towards awarding off of predatory factors inherent in economic backwardness of nations. This accounts for the rising rate of cyber related crime in Nigeria and other parts of the world.

Education and Misuse of Modern Technologies for Cybercrime by Youths

Education is the process through which the experience of generations, comprising knowledge, skills and attitudes are transmitted to individuals who are member of the community. Concept change, attitudes and skills undergo alterations, interests and values face revisions and life itself undergoes a continuous modification of experience. In this context, education is the process of assisting the learner to adjust to ever changing behaviour and adaptation to perceived values.

Education is the most vital weapon for literacy. The consequences of illiteracy are many and harmful in several respects. As well as affecting illiterate individuals themselves in their daily lives and often jeopardizing their future, which has a significant effect on individual socially and psychologically. The consequences of illiteracy on individual include limited ability to obtain and understand essential information. Some youths engage in cybercrime activities due to limited information leading to low self-

esteem ad isolation which may result to the misuse of modern technologies for cybercrime.

Since literacy is an essential tool for individuals especially the youths to fill vacant positions in the society, individuals without an adequate level of literacy cannot fit in and may resort to cybercrime activities to increase their socioeconomic status. Youths who are gainfully employed may participate in cybercrime activities but research have shown that illiterate youths are more prone and attracted to criminal tendencies.

The mass media can be a tool for encouraging youths in participating in cybercrime activities through programmes that may suggest the positive side of involvement in cybercrime activities.

Role of Gender and Participation in Cybercrime

Only few cybercrimes are committed by females, but it is important to understand the relationships between gender and cybercrime to inform crime prevention strategies because from all indications, it appears that cybercrime is predominantly conducted by males (Bachmann, 2010' Chamtter 1995, Turgeman – Goldchmidt, 2005), with Chemitter (1995) reporting that female hackers are perceived with either complete disdain or with high regard by general hacking community. Taylor (1999) states that the gender ratio at hacking conferences is approximately one female to every one hundred

males and that often females are often transiently involved in the hacker subculture. Hollinger's (1993) study of one college students found that 5.2 percent of males and 1.8 percent of females admitted to having accessed another's computer account or files without permission.

This gender imbalance in cybercrime resembles the gender imbalance in offending more generally. It is well established that the frequencies and severity of crimes committed by females are lower than their male counterpart. This fact holds across self-reported and official data (Gelsthorpe and Wright, 2015; Schwartz et al, 2009; Steffensmeier and Allen, 1996) and crime types, such as gang violence (Miller and Decker, 2001). In addition to lower frequencies and severity, females tend to play minor roles even when participating in more masculine environment such as drug markets (Maher and Daly, 1996). However, there is a shift away from using traditional theories in understanding the experiences and interaction of female offenders because those theories were criticized to be insufficient to account for the gender imbalance as most of the theories are derived or developed based on male offenders (Smith and Petermoster, 1987). Thus, one approach is to analyze events and experiences of female offenders to understand their pathway in criminal behaviours.

With gender and cybercrime, pathways to crime provide insight on the gender imbalance in cybercrime by addressing two issues. The first issue is the effects on involvement in crime. In their model, Heimer and De Coster (1999) incorporate a cultural definition of gender in addition to structural positions and favourable definitions from differential association theory. Findings suggest that the process through which favourable definitions are learned is structured and influenced by gender. Bottcher (2001) conceptualises both gender and delinquency in terms of social practices. The overlap in the social practices explains the discrepancies in females' and males' pathway to crime. For example, the males in the interview were given more freedom to explore outside the house whereas females were more restricted in terms of supervision and chores.

The underpinning philosophy guiding women-crime engagement in research remains the realities of women's lives that if firmly located in the social, economic, political, educational and relational aspects of women's encounter with the physical world. In terms of circumstances and characteristics of criminal acts, women were found to be more represented in property offenses and constitutes nearly one fifth of alcohol motivated offenders (Kassebaum, 1999). However, they are more likely than male offenders to use drug and including addiction to more serious drugs

(Kassebaum, 1999). They were also found to be less participant in violent offences. Research has thrown light on why female criminality receives little attention in crime studies. In his leading argument, Pollack expatiated that women's nature is shrouded in falsehood though their posture often appearing innocent within the context of transient encounter but it is absolutely laden with innate secrecy to conceal their male and female crime are traceable to benefits of modernity that are located in the expansion of communication technologies, mass enlightenment, access to paid employment, viability in the public realm due to roles of liberation movements, expansion of freedom to women, equality and host of other factors combined to increase female opportunity to engage in crime. From Adler's view, due to greater pressure on women as a result of their occupation in the hitherto men's domain, women are becoming more susceptible to the same crimogenic forces that men faced (Adler, 1975). Her argument tilts towards the establishment of equity or at best an increase in female offending as compared to male offending. She summarized it this way:

> Women are no longer indentured to the kitchens, baby carriages or bedrooms of America… allowed their freedom for the first time, women… by the tens of thousands – have chosen to desert those kitchens and plunge exuberantly into the formerly all male quarters

> of the working world… In the same way that women are demanding equal opportunity in the field of legitimate endeavor, a similar number of determined women are forcing their way into the world of major crimes. Pp. 12-13.

The fundamental basis of more involvement hinged primarily on power relations. And reporting further on devolution of power associated with modernity, scholars exonerate several other factors that are not responsible for movement towards equity in both sexes offending. On risk related factors explaining differences in crime involvement, several studies have found that there exists no genetic and environmental factors pre-disposing both sexes to crime (Sluske et al, 1997: Gottesman et al, 1997; Baker et al, 1989 and Cardoret et al, 1995). Although this submission on liberation and parity in power possession promoting crime was reduced to over assumption (Boritch, 1992), it is noticed in the era of modernity that women were observed to be committing more crimes and young girls are joining gangs in record numbers (Esbensen and Deschenes, 1998). Contrary to Adler's view on the consistently closure of gap between male and female offending, Steffensmeier (1980) posited that it is quite true that female involvement in crime is on the increase but this remains insufficient to meet up with the magnitude attained in male related crimes. Further posturing on the increment in female crime participation, Silvestri and Crother-Dowey

(2008:26) mentioned that the overriding consensus within criminology remains that while women do commit a broad range of offenses, they commit less than men and are less dangerous and violent than their male counterparts.

Thus, having established the synergy between male-female criminality, it is quite central to situate the focus of this review as it affects the present concern. The current effort attempts the expansion of literature by supporting the argument that females are not completely passive, un-ambitions and restricted into the private realm in this technological age. Females are rapidly advancing in both conventional and non-conventional arenas to catch up with their male counterparts even in environment of crime. Male and female exertion of violence is now gradually on the increase, and participation of both sexes in technological driven crimes is visibly becoming the norm (Miller and White, 2003). Participation in technologies crime have been traced to the quest after economic cum social gains. Research has shown that women lawbreakers are economically active and creative decision makers who usually ruminate on how best to generate gains and yet often faced with contradictory choices (Maher, 1997). In most cases, women are left to bowl alone and in their quest to survive, this situation translates into high predisposability to crime. They are constantly

faced with the dilemmic events of selecting between contended with and operating within the gendered norm and favouring anti-social conducts. Women's existence is quite vital to complementary role in crime chain and in more especially fraud which has been their traditional domain. The most unique advantage that girls have over their boys counterpart in the environment of electronic driven fraud consist of the possession of verbal proficiency needed to perfect the pranks required to secure success in Internet Fraud (Siegel, 2010: 54). In terms of arrest rate, it is requited that female arrest rate seemed to be increasing at a faster pace and it was believed that there may be convergence between female and male arrest rate for cyber fraud but relatively to the ratio of gender participation. Although, the United Nations (2005) lamented the inequality of access to ICT facilities for women, it should be noticed that a few representation of women in ICT does not insulate them from crime participation in the cyber arena.

Cybercrime Activities among Youths in Nigeria

From research and information gathered, cybercrime is prevalent in Nigeria, especially among the youths who no longer see anything wrong with cybercrime activities. Some youths even protest against law enforcement agencies in solidarity with their friends and colleagues and abandon academic activities. The following reports are some of the

documented evidences of youths' involvement in cybercrime activities in Nigeria.

The Economic and Financial Crimes Commission (EFCC) on Thursday, arraigned a suspect declared wanted by the United States Federal Bureau of Investigation before a State High Court on a five-count charge of cybercrime and other related offences. Although the accused pleaded not guilty, it was gathered that he got N60m from the crime via Western Union Transfer. He carried out the crime through a false identity and pretense. The case was adjourned till 9th of October for the commencement of trial. Similarly, a judge sentenced one suspect of Internet crime to six months' imprisonment for impersonation. The suspect who presented himself as a white man who was into supply of construction equipment defrauded his victims through the Internet. The judge ordered that the convicts laptop and telephone be forfeited to the Federal Government (Oluwatoyin Omojiyugbe and Tunde Oyekola: Punch News, September 27, 2019).

According to Ademola Babalola (2019) the EFCC on Wednesday 7th August 2019 arrested 29 men suspected to be involved in Internet-related fraud. Popularly known as "yahoo boys", the suspects were arrested on Akoto Estate, Ehebu area of Ibadan, Oyo State. They were rounded up during an early morning raid by operatives of the Commission. Among the

items recovered from the suspects were eight (8) exotic cars, expensive phones and laptops as well as documents suspected to have been used for illicit deals. According to the anti-graft agency, the suspects will be charged to court as soon as investigation is concluded.

In what will be referred to by many as notable endeavour commercial motorcyclist in Abraka prevented the arrest of a young man by the Special Anti-Robbery Squad (SARS) operatives of Delta State Police, who they suspected to be an Internet fraudster. Despite efforts by the officers to disperse the crowds, the bike men were unshaken in their resolve to stop them from taking the suspect away, claiming that they make more of their money from the yahoo boys. The youths also complained that this set of operatives has been terrorising commuters, especially young men driving flashy cars. In most cases, they forcefully take them to ATM after checking their account balance with their phones. “Their activity is giving the Nigerian police a bad image, the source who pleaded anonymity added” (Ovie Okpere: Punch News, 30 September, 2019).

In another development, Wale Odunsi (2019) reports that the operatives of the EFCC advance fee section in Abuja arrested 22 suspected Internet fraudsters during an early morning raid in Sapele, Delta State on Friday May 17, 2019. Similarly, EFCC operatives from Abuja had arrested

two suspected internet fraudsters in Ughelli, Delta State on Thursday 16th May, 2019. Items recovered from the suspects include laptops, computers, Iphones, Phones, ATM cards and three exotic cars BENZ C350, BENZ ML350 and Chrysler 300. The suspects who made useful statements would soon be charged to court. Meanwhile, the EFCC has filed an eleven-count charge bordering on fraud against a Nigerian Musician, who is known for glorifying Internet fraud. He was arrested on his birthday, just a few days after the release of a song "am I a yahoo boy".

Consequently, students of the Ekiti State University, Ado Ekiti on Wednesday 7th August 2019 trooped to the streets to protest alleged arrest of their colleagues by operative of the EFCC. A couple of weeks ago, over 40 youths some of whom were students of higher institutions were arrested in Ado-Ekiti by EFCC and transferred to Ibadan, Oyo State for alleged cyber fraud. They blocked the highway, thereby causing traffic and long queues of vehicle along that route. Daily Post Prince reports that the protest affected the academic activities as most of the lecturers and other staff could not access the campus because the students took over Ado-Ekiti dual carriage way for over two hours.

Victor Ogunyinka (2019) reports that the EFCC, Abuja Zonal Office, arrested 10 suspected Internet fraudsters, following intelligence report of

their suspicious activities. They were arrested at Kanu and Mpape settlements on February 7, 2019. Items recovered from them include three Mercedes Benz cars, five laptop computers, 10 handsets, ATM cards and other incriminating documents.

It therefore suggests the fact that the society encourages cybercrime activities either because they are beneficiary directly or indirectly or for a mere show of solidarity with neigbhours and friends. They prevent suspects from being arrested, by law enforcement agents which also hinders investigation and prosecution.

Legislation on Cybercrime in Nigeria

The rise in cybercrime has compelled the Nigerian government to legislate against it.

Nigeria's Cybercrime Act 2015

The Cybercrime Act is an official statement or document that controls the use of the Internet for cybercrime. The Act makes it an offence for any person or group of persons to engage in malicious or deliberate spread of virus or malware that can cause damage to critical information in private, public or cooperate organizations. In Nigeria, there are different penalties for different cybercrimes and it is to check the illegal transactions carried out by

cybercriminals. The following are some of the cybercrime Act 2015 in Nigeria.

1. The Nigerian Cybercrime Act 2015 gives the President the power to designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well-being of its citizens, as constituting Critical National Information Infrastructure and to implement procedures, guidelines, and conduct audits in furtherance of that.
2. The Nigerian Cybercrime Act 2015 prescribes the death penalty for an offence committed against a system or network that has been designated critical national infrastructure of Nigeria that results in the death of an individual (amongst other punishments for lesser crimes).
3. Under the Cybercrime Act 2015 in Nigeria, hackers, if found guilty of unlawfully accessing a computer system or network are liable to a fine of up to N10 million or a term of imprisonment of 5 years (depending on the purpose of the hack). The same punishment is also meted out to Internet fraudsters who perpetuate their acts either by sending electronic messages, or accessing and using data stored on computer systems.

4. The Cybercrime Act 2015 makes provision for identity theft with the punishment of imprisonment for a term of not less than 3 years or a fine of not less than N7 million or to both fine and imprisonment. An example of identity fraud would be the individual who impersonated Chief Bola Tinubu on facebook and was apprehended recently by the police.

5. Specifically creates child pornography offences with punishments of imprisonment for a term of 10 years or a fine of not less than N20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others producing, procuring, disturbing, and possession of child pornography.

6. Outlaws Cyber-stalking and Cyber-bullying and prescribes punishment ranging from a fine of not less than N2 million or imprisonment for a term of not less than 1 year or to both fine and imprisonment, up to a term of not less than 10 years or a fine of not less than N25 million or to both fine and imprisonment; depending on the severity of the offence.

7. The Nigerian Cybercrime Act 2015 prohibits cybersquatting, which is registering or using an Internet domain name with bad faith intent to

profit from the good will of a trademark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than N5 million or to both fine and imprisonment.

8. Forbids the distribution of racist and xenophobic materials to the public through a computer system or network (e.g facebook and twitter), it also prohibits the use of threats of violence and insulting statements to persons based on race, religion, colour, descent or national or ethnic origin. Persons found guilty of this are liable on conviction to imprisonment for a term of not less than 5 years or to a fine of not less than N10 million or to both fine and imprisonment.

9. The Cybercrime Act 2015 mandates that service providers shall keep all traffic data and subscriber information having due regard to the individual's constitutional Right to privacy and shall take appropriate measures to safeguard the confidentiality of the data retained processed or retrieved.

10. Allows for the interception of electronic communication, by way of a court order by a judge, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably

required for the purposes of a criminal investigation or proceedings (Nigeria Cybercrime Law, 2015).

Preventive Measures for Cybercrime and the Misuse of Modern Technologies by Nigerian Youths

Internet users should exercise some of the following basic precautions to avoid becoming victims of cybercrime and the misuse of modern technologies.

- Use a full service Internet security site. For instance, Norton security provides real time protection against existing and emerging malware including ransomware and viruses and help protect private and financial information online.
- Use strong passwords: repeating passwords on different sites and changing them regularly can create doors for cybercrime activity. Using complex password of a combination of at least 10 letters numbers and symbols can be better.
- Keep software updated: This is important when operating system and Internet security software. Criminals frequently use known exploits, or flaws in software to gain access to systems.
- Manage Social Media Settings: Personal and private information should be locked down regularly. Social engineering cyber criminals can often get personal information with just a few data point.
- Strengthen Home Network: It's a good idea to start with a strong encryption password as well as virtual private network. Asian Venture

Philanthropy Network (AVPN) will encrypt all traffic leaving devices until it arrives its destination. If cyber criminals manage to hack communication they would intercept the encrypted data.

- Talk to children about the danger of the misuse of the internet: As early as possible, children and youths should be taught the dangers cybercrime activities and they should be educated on the need to open up if they are experiencing any kind of online harassment, stalking or bullying.
- Keeping up to date on major security breaches can be of great advantage. If an account on a website has been impacted by a security break, find out what information the hackers accessed and change password immediately.
- Measure should be taken towards protection against identity theft. Identity theft occurs when someone wrongfully obtains personal data in a way that involves fraud or deception, typically for economic gain. A Virtual Private Network (VPN) can help to protect the data sent or receive online.
- Protect personal identities everywhere. Some personal information can be accessed by criminals anywhere. Therefore, keep all personal

details off social media e.g travel plan and using a VPN when accessing the Internet can be of help.

- Most kids are aware of the Internet, parent should advice and supply basic information to them on identity theft as they are sometimes the target of most cyber criminals.
- When it is discovered that one is a victim of cybercrimes the police should be put on notice, and in some cases the Federal Bureau of Investigation (FBI) and Federal Trade Commission. This is important even if the crime seems minor. The information may assist authorities in their investigations or may help to stop criminals from taking advantage of other persons subsequently. Such information may include contacting the companies and banks where the fraud occurred. Place fraud alerts and get credit reports and reporting identity theft to the FTC.

Summary of Related Literature

The study examined the misuse of modern technologies for cybercrime among youths. It was revealed that much of Western history on the dominant theory of crime was the demonic perspective. The demonic perspective was dominant through the 1700s, when it was challenged during the Age of Enlightenment by a group of individuals who came to be known

as the “classical” criminologists. The essential ideas of “classical theory” are quite simple. Individuals are rational beings who pursue their own interests, trying to maximize their pleasure and minimize their pain. And unless they are deterred by the threat of swift, certain and appropriately severe punishment, they may commit crimes in their pursuit of self-interest.

Several theories have fingered to a lot of reasons why youths engaged in cybercrime, as it is the focus of this study. They attributed it to parents and the society, self-control, social class and race, etc. Various violent cybercrime have been identified which includes, cyber terrorism, cyber extortion cyber stalking, cyber bullying, pornography, fraud-identity theft, drug trafficking deals, logic bombs, password sniffing, wire-tapping/illegal interception telecommunication.

However, other non-violent cybercrime including online prostitution, gambling, illegal drug sales on the internet and cyber laundering. Several sociological theorists that spanned through the classical, modern and postmodern periods were used in this study. Although, all of them in the different opinions have also come to agree that cybercrime pose a threat to the society. It is also against this background that the effects of cybercrime on youths were discussed. These includes lack of interest in academic, disconnection from family members even untimely death.

Finally, the study proffers preventive measures for cybercrime and the misuse of modern technologies. These include the use of strong passwords, repeating passwords on different sites and changing them regularly can create doors for cybercrime activities. The use of complex password of a combination of at least 10 letters number and symbols can be better. Secondly, keeping software updated is important when operating system and internet security software. Cybercriminals frequently use known exploits, or flaws in software to gain access to systems. And lastly personal and private information should be locked down regularly.

CHAPTER THREE

METHODOLOGY

This chapter presents the method and procedures adopted in carrying out the study under the following sub-headings: Research Design, Population of the Study, Sample and Sampling Procedure, Research Instrument, Validity of the Instrument, Reliability of the Instrument, Method of Data Collection and Method of Data Analysis.

Research Design

The study adopted the descriptive survey research design based on correlational type. Survey design is considered most appropriate for this study because the data collected can be generalized for all the population and the subject of investigation centres on individuals' opinions, attitude and perceptions hence the variables were not manipulated. This study elicited opinion and information from undergraduates and postgraduate students in the University of Benin.

Population of the Study

The population for the study is forty-three thousand, seven hundred and seven-two (43,772) which comprises thirty-nine thousand, two hundred and forty-three (39,243) undergraduates and four thousand, five hundred and twenty-nine (4529) postgraduates. There are sixteen (16) faculties in the University of Benin which include Agriculture, Arts, Basic Medical Science,

Dentistry, Education, Engineering, Environmental Sciences, Law, Life Sciences, Management Sciences, Medicine, Pharmacy, Physical Sciences, Social Sciences, Veterinary Science and other services.

Table 1: Distribution of Undergraduates and Postgraduate Students in University of Benin

S/N	Faculty	No. of Department	Number of Students				Total
			Undergraduate		Postgraduate		
			Male	Female	Male	Female	
1	Agriculture	06	900	1156	143	77	2276
2	Arts	08	2197	3513	158	91	5959
3	Basic Medical Science	07	773	1175	152	183	2283
4	Dentistry	06	119	49	-	-	168
5	Education	08	2993	4376	351	430	8150
6	Engineering	07	3308	503	725	100	4636
7	Environmental Sciences	04	462	134	-	-	596
8	Law	04	414	575	57	45	1091
9	Life Sciences	07	2193	2895	237	224	5549
10	Management Sciences	04	1563	1568	171	125	3427
11	Medicine	18	542	253	40	38	873
12	Pharmacy	06	582	412	141	109	1244
13	Physical Sciences	06	1703	1346	282	91	3925
14	Social Sciences	06	1703	1333	281	142	3459
15	Veterinary Med	02	-	-	-	-	-
16	Other services	05	-	-	41	95	36
	Total	**104**	**19955**	**19288**	**2779**	**1750**	**43772**

Source: Department of Academic Planning, Students Affairs Division, UNIBEN (2019)

Sample and Sampling Procedure

The sample for the study was four hundred and two (402) undergraduates and postgraduate students selected through multi-stage sampling procedure

Step I: Thirty percent 30% of all the sixteen (16) faculties was sampled which amount to five (5) faculties.

Step II: Five faculties was randomly selected which are faculties of Arts, Education, Social Sciences, Physical Sciences and Agricultural Science.

Step III: In selecting the sample for the study twelve (12) students were purposively selected from each department across the sampled faculties. For this purpose six students each sampled on the undergraduates and postgraduates students from the select departments. Table 2 shows the number of students drawn from the various faculties and departments based on the proportion of the total.

Table 2: Sample Distribution of Students

S/N	Sampled Faculties	Department	No. of Department	No. of Sampled Students		Total No. of Students
				400 level	Masters	
1		Agricultural Economics and Extension Services		6	6	72
		Animal Science		6	6	
		Crop Science		6	6	
	Agriculture	Agriculture and Fishery Management	06	6	6	
		Forestry Resource and Wild Life Management		6	6	
		Solid and Land Resource Management		6	6	
2		English and Literature		6	6	
		Fine and Applied Arts		6	6	
		Foreign Languages		6	6	
		History and International Studies		6	6	
	Arts	Linguistics Studies	08	6	6	96
		Philosophy		6	6	
		Religion		6	6	
		Theatre Art and Mass Communication		6	6	
3		Adult and Non-formal Education		6	6	
		Curriculum and Instructional Technology		6	6	
		Educational Evaluation and Counselling Psychology		6	6	
		Educational Management		6	6	
	Education	Educational Foundations	08	6	6	90
		Human Kinetics and Sports Science		6	6	
		Health, Safety and Environmental Education		6	6	
		Vocational and Technical Education		6	6	
4		Chemistry		6	6	
		Geology		6	6	
		Mathematics		6	6	
	Physical Science	Computer Science	06	6	6	72
		Physics		6	6	
		Statistics		6	6	
5		Economics and Statistics		6	6	
		Geography and Regional Planning		6	6	
	Social Science	Political Science		6	6	72
		Sociology and Anthropology	06	6	6	
		Social Works		6	6	
		Public Administration				
						408

Finally, the researcher purposively drew equal number of six (6) students each from 400 level undergraduates and postgraduates from each department. For example, the faculties of Agriculture, Physical Science and the Social Sciences 36 students each were drawn from 400 level and postgraduate degree while in faculties of Arts and Education, 48 students each were draw from 400 level and postgraduates. In all a total of four hundred and two (408) students became the respondents of the study in the University of Benin.

Research Instrument

The research instrument used for this study is a questionnaire developed by the researcher titled **"Misuse of Modern Technologies for Cybercrime by Youths Questionnaire" (MMTCYQ)** made up of fifty (50) questions divided into two sections. Section A elicited bio-data information which consists of gender, age, location, faculty, department and academic level of respondents (students) while Section B contains items on a scale of misuse of modern technology for cybercrime by youths. The items in Section B were structured on a five point likert scale of "Strongly Agree" "Agree" "Undecided" "Disagree" and "Strongly Disagree".

Validity of the Instrument

The self-designed questionnaire was validated by the researcher's supervisor in the Department of Educational Foundations and two experts in Measurement and Evaluation, Faculty of Education, University of Benin. Their inputs and corrections were effected before producing the final draft of the instrument.

Reliability of the Instrument

The reliability of the instrument was determined through a test re-test technique for a group of twenty (20) students from the Faculty of Law on the misuse of modern technology by youths with an interval of two weeks. The selected students were not part of the main study. Thereafter the Pearson Product Moment Correlation Co-efficient (Pearson, r) was used to obtain a reliability value of 0.96.

Method of Data Collection

The instrument was administered by the researcher and two trained research assistants. A total of four hundred and eight (408) copies of the questionnaire were administered and retrieved which amounted to one hundred percent 100% of return.

Method of Data Analysis

The data was analyzed using frequency and percentages for the respondents' bio-data, while mean and standard deviation were used to answer the research questions. The hypotheses were tested using chi-square statistics for hypothesis 4 that was tested using t-test of independent samples.

The criterion for `agree' and `disagree' was set at mean values of 3.00 and above as `agree', while mean values below 3.00 was `disagree'. The mean criterion value was derived, thus: SA=5, A=4, U=3, D=2, SD=1, $5+4+3+2+1 = \frac{15}{5} = 3.00$.

CHAPTER FOUR

PRESENTATION OF RESULTS AND DISCUSSION OF FINDINGS

This chapter is concerned with the presentation of data analysis, interpretation of results and discussion of findings. It was undertaken to find out the misuse of modern technologies for cybercrimes by youths: The University of Benin.

Answer to Research Questions

The data analysis for the research questions were carried out using mean and standard deviation.

Table 1: Percentage Distribution of Respondents by Gender

Gender	Frequency	Percentage
Male	207	50.7
Female	201	49.3
Total	408	100.0

The data presented in Table 1 showed that there were 207 male students who indicated their gender and this represents 50.7 percent respondents. Similarly, there were 201 female students who indicated their gender, representing 49.3 percent.

Table 2: Percentage Distribution of Responses by Age

Age (Years)	Frequency	Percentage
Below 18 years	42	10.3
18-20 years	133	32.6
21-24 years	81	19.9
25-30 years	63	15.4
31.35 years	19	4.7
35 years and above	70	17.2
Total	408	100.0

The data presented in Table 2 shows that there were 42 students within the age range of below 18 years and this represent 10.3 percent respondents. Also, 133 students were within the age range of 18-20 years, representing 32.6 percent. Similarly, 81 respondents were within the age range of 21-24 years and this represents 19.9 percent. In the same vein, 63 students fell into the age bracket of 25-30 years which accounted for 15.4 percent. Consequently, 19 students representing 4.7 percent were in the age range of 31-35 years. Lastly, 70 students were covered between 35 years and above, representing 17.2 percent.

Table 3: Percentage Distribution of respondents by Location

Location	Frequency	Percentage
Urban	344	84.3
Rural	64	15.7
Total	408	100.0

The data as presented in Table 3 showed that 344 students which represented 84.3 percent were located in the urban areas, while, 64 students were based in rural areas, representing 15.7 percent.

Table 4: Percentage Distribution of Respondents by Academic Level

Academic Level	Frequency	Percentage
400 level	204	50.0
Masters	204	50.0
Total	408	100.0

The results presented in Table 4 revealed that both 400 level and master's students were same in number, i.e 204 apiece which accounted for 50 percent each.

Table 5: Percentage Distribution of Respondents by Faculty

Faculty	Frequency	Percentage
Arts	96	23.5
Agriculture	72	17.6
Education	96	23.5
Physical Sciences	72	17.6
Social Sciences	72	17.6
Total	408	100.0

From the results in Table 5, it is revealed that the faculties of Arts and Education both had 96 students representing 23.5 percent who participated in the study respectively. Similarly, Faculties of Agriculture, Physical Sciences and the Social Sciences had 72 students each which represents 17.6 percent each that took part in the study respectively.

Table 6: Percentage Distribution of Respondents by Department

S/N	Department	Frequency	Percentage
1	Adult and Non-Formal Education (ADULT)	12	2.9
2	Agricultural Economics and Extension (AGR ECONS & EXT)	12	2.9
3	Animal Science (ANIMAL SCI)	12	2.9
4	Aqua and Fishery Management (AQUA & FISH MGT)	12	2.9
5	Chemistry (CHM)	12	2.9
6	Curriculum and Instructional Technology (CIT)	12	2.9
7	Computer Science (COMP. SCI)	12	2.9
8	Crop Science (CROP SCI)	12	2.9
9	Educational Foundations (DEF)	12	2.9
10	Educational Management (DEM)	12	2.9
11	Economics and Statistics (ECO STAT)	12	2.9
12	Educational Evaluation and Counselling Psychology (EECP)	12	2.9
13	English and Literature (ENG & LIT)	10	2.5
14	Fine and Applied Arts	13	3.2
15	Forest Resources and Wildlife Management	12	2.9
16	Foreign Languages	12	2.9
17	Geography and Regional Planning	12	2.9
18	Geology	12	2.9
19	History and International Studies	13	3.2
20	Human Kinetics and Sports Science (HKS)	12	2.9
21	Health, Safety and Environmental Education (HSE)	12	2.9
22	Linguistics	12	2.9
23	Mathematics	12	2.9
24	Philosophy	12	2.9
25	Physics	12	2.9
26	Political Science	12	2.9
27	Public Administration	12	2.9
28	Religion	12	2.9
29	Sociology and Anthropology	12	2.9
30	Social Work	12	2.9
31	Soil and Land Resources Management	12	2.9
32	Statistics	12	2.9
33	Theatre Arts	6	1.5
34	Theatre Arts/Mass Communication	6	1.5
35	Vocational and Technical Education (VTE)	12	2.9
	Total	408	100.0

From the results in Table 6, it is revealed that departments of ADULT, AGRIC, ECONS & EXT, ANIMAL SCI, AQUA & FISH MGT, Chemistry, CIT, COMP SCI, CROP SCI, DEF, DEM, ECO STAT, EECP, Forest Resources and Wildlife Management, Foreign Languages, Geography and

Regional Planning, Geology, HKS, HSE, Linguistics, Mathematics, Philosophy, Physics, Political Science, Public Administration, Religion, Sociology and Anthropology, Social Work, Statistics, Soil and Land Resources Management and VTE all had 12 respondents each which represented 2.9 percent respectively. In the same way, Departments of Fine and Applied Arts and History and International Studies had 13 respondents each which represents 3.2 percent respectively. The Department of English and Literature accounted for 10 students, representing 2.5 percent. Finally, the Departments of Theatre Arts and Mass Communication had 6 respondents each, representing 1.5 percent respectively.

Research Questions 1: What are the causes of the misuse of modern technology for cybercrime activities by youths in Nigeria?

Table 7: Mean Standard Deviation of responses on the Misuse of Modern Technology for Cybercrime Activities by Nigerian Youths

S/N	Item Statements	Mean	Std. Dev.	Remark
1	Unemployment is a motivating factor for the involvement of youths in cybercrime activities	4.26	0.979	Agree
2	Youths participation in cybercrime majorly to get more money	4.52	0.694	Agree
3	Poverty is a major factor for the involvement of youths in cybercrime	4.12	1.029	Agree
4	The Nigerian youths appreciates cybercrime as an opportunity for wealth and affluence	4.14	1.009	Agree
5	The contemporary Nigerian society appreciates and applaud dividends from cybercrimes and cybercriminals	3.47	1.246	Agree
6	Parental conflict can be responsible for the involvement of youths in cyber related crimes	3.37	1.178	Agree

The data in Table 7 shows that the mean responses ranged from 3.37 to 4.52, while the standard deviation ranged from 0.694 to 1.246. The mean values show that the respondents agree to the six causes of misuse of modern technology for cybercrime activities by youths, while the relative low values of the standard deviation revealed that the respondents are in consensus with the causes of the misuse of modern technology for cybercrime activities.

Research Question 2: What is the effect of the misuse of modern technology for cybercrime on individuals and the society?

Table 8: Mean and Standard Deviation of responses on the Effect of Misuse of Modern Technology for Cybercrime on Individuals

S/N	Item Statements	Mean	Std. Dev.	Remark
7	Cybercrime has negative effect on the Nigeria society	4.47	0.875	Agree
8	The misuse of modern technologies by youths has a positive effect on them	2.72	1.470	Disagree
9	Cyber-crime is a legal method for wealth creation	2.08	1.454	Disagree
10	Involvement in cybercrime activities can affect youths academic pursuit and achievements	4.17	1.125	Agree
11	Cybercrime activities influences youths interpersonal relationship negatively	3.96	1.026	Agree
12	Cybercrime activities affects social behaviour among Nigerian youths	4.14	0.956	Agree

The results in Table 8 indicate that the mean values ranged from 2.08 to 4.47 and the values of the standard deviation ranged from 0.875 to 1.470. The table shows that the respondents agreed to items 7,10,11 and 12 which bordered on the fact that cybercrime activities can have a negative effect on

Nigerian youths, while they disagreed with items 8 and 9 that portrayed cybercrime in a positive light. However, an average mean of 3.59 revealed that cybercrime activities can impact negatively on youths in the areas of academics, interpersonal relationships, social behaviour, and so on. The low values of the standard deviation revealed that the responses do not deviate far from each other.

Research Question 3: Does non-prosecution of cybercriminals by government and law enforcement agents encourage youth participation in cybercrime activities in Nigeria.

Table 9: Mean and Standard Deviation of responses on Cybercriminals activities due to Non-prosecution by Government Agencies

S/N	Item Statements	Mean	Std. Dev.	Remark
13	Refusal to lodge complaints about cybercrime to relevant authorities help to encourage more involvement in cybercrime activities	4.15	1.023	Agree
14	Instability of government policies encourages youth involvement in cybercrime activities	4.27	0.868	Agree
15	The law enforcement agents in most cases encourages cybercriminals through lack of proper investigation	4.16	0.895	Agree
16	Failure to prosecute cybercriminals can encourage more participation in cybercrime activities	4.39	0.795	Agree
17	The absence of effective punishment on cybercriminals encourage more participation	4.39	0.816	Agree

The data presented in Table 9 revealed that the mean values ranged from 4.15 to 4.39 and the values of the standard deviation ranged from 0.795 to 1.023. The table shows that the respondents agree to the five items as regards non-prosecution of cybercriminals by government and law enforcement agents encouraging Nigerian youths' participation in cybercrime activities. The low values of the standard deviation reveal that their responses do not deviate significantly from each other.

Research Question 4: Is there any relationship between peer group influence and youths' involvement in cybercrime activities in Nigeria?

Table 10: Mean and Standard Deviation of responses on Relationship between Peer Group Influence and Youths' Involvement in Cybercrime Activities

S/N	Item Statements	Mean	Std. Dev.	Remark
18	Sociological influence can encourage youths' involvement in cybercrime	4.28	0.808	Agree
19	Youths' who are not under direct control or surveillance of their parents are more prone to participation in cybercrime activities	3.72	1.218	Agree
20	Criminal behaviours are learned and not inherited	4.26	0.845	Agree
21	The principal part of learning criminal behaviour occur within intimate personal groups	4.27	0.824	Agree
22	Lack of self-control is a driving force behind youths' participation in cybercrime activities	4.14	0.941	Agree
23	Association with cybercriminals can influence youths' involvement in cybercrime activities	436	0.739	Agree

The data as presented in Table 10 revealed that the mean values of the standard deviation ranged from 0.739 to 1.218. The table showed that the respondents agreed to the six items as concerns relationship between peer group influence and youths' involvement in cybercrime activities, while the relative low values of the standard deviation showed that the respondents are in consensus with the results.

Research Question 5: Is there any relationship between the knowledge of the internet and cybercrime activities among youths in Nigeria?

Table 11: Mean and Standard Deviation of responses on Knowledge of Internet and Cybercrime Activities among Nigerian Youths

S/N	Item Statements	Mean	Std. Dev.	Remark
24	There is a direct link between the knowledge of the internet and cybercrime activities	3.83	1.081	Agree
25	Most youths involve in cybercrime because they feel that the internet is a safe place for criminal activities	3.68	1.111	Agree
26	Overuse of the internet harms youths academic and social activities	2.08	1.454	Disagree
27	Environment and locality influences youths' involvement in cybercrime activities	4.11	0.876	Agree
28	Cybercriminals are mainly from the urban areas or centres	3.53	1.201	Agree

The data presented in Table 11 indicated that with an average mean of 3.82 the respondents agreed to the five items in relation to the knowledge of the internet and cybercrime activities among Nigerian youths. The relative low values of the standard deviation reveal that the responses do not deviate significantly from each other.

Research Question 6: Is there any relationship between the socio-economic status of Nigerian youths and their involvement in cybercrime activities in Nigeria?

Table 12: Mean and Standard Deviation of responses on the socio-economic status of Nigerian Youths and Cybercrime Involvement

S/N	Item Statements	Mean	Std. Dev.	Remark
29	Socio-economic factor influence youths' participation in cybercrime activities	4.16	0.895	Agree
30	Striving for social status is one reason youths participate in cybercrime activities	4.26	0.826	Agree
31	Illiterate youths with low educational background are easily influenced towards negative tendencies	3.99	1.031	Agree
32	Occupational background can influence youths participation in cybercrime	3.68	1.098	Agree
33	Youths who are not gainfully employed participate more in cybercrime activities	3.93	1.081	Agree

The result presented in Table 12 indicated an average mean value of 4.00 which shows that the respondents agreed to all the five items regarding the relationship between socio-economic status and youths' involvement in cybercrimes. Also, the corresponding low values of the standard deviation mean that their responses do not deviate significantly from each other.

Research Question 7: Is there any significant difference in gender and youths' participation in cybercrime activities in Nigeria?

Table 13: Mean and Standard Deviation of responses on Gender and Youths' Participation in Cybercrime Activities

	Gender	N	Mean	Std. Dev.
Participation	Male	207	16.99	3.740
	Female	201	18.01	4.903

The data in Table 13 showed that the mean for males is 16.99 and that for females is 18.01. Thus, the females have a higher mean than the male students. This means that the females were more involved in cybercrime activities than their male counterparts. Though this is surprising as it contradicts most researches related to this study. However, this is based on the data as provided by respondents as it may be that they are not so sure of the information required of them.

Table 13b:

S/N	Item Statements	Mean	Std. Dev.	Remark
34	Female cybercriminals are not volatile as their male counterparts	3.68	1.221	Agree
35	Participation of the males are more prominent than their females counterpart in cybercrime activities	4.32	0.884	Agree
36	Females participation in cybercrime activities just for fun and entertainment	2.61	1.188	Disagree
37	Gender is a major factor in the participation of cybercrime activities	2.99	1.312	Disagree
38	Deviant behaviours are rampant males	3.75	1.91	Agree

The results of Table 13b indicated that the mean values ranged from 2.61 to 3.75, while the standard deviation values ranged from 0.884 to 1.312. The result showed that the respondents agreed to items 34, 35 and 38 which buttressed the fact that males are more inclined to cybercrime and deviant behaviours than their female counterparts, while they disagreed with items 36 and 37.

Research Question 8: Is there any relationship between family and parents socio-economic background and youth involvement in cybercrime activities in Nigeria?

Table 14: Mean and Standard Deviation of responses on Family Socio-economic Background and Youths' Involvement in Cybercrime

S/N	Item Statements	Mean	Std. Dev.	Remark
39	Parents socio-economic background can influence youths' participation in cybercrime activities	4.01	0.951	Agree
40	Youths from poor family background are more prone to cybercrime activities because they lack finance for their basic needs	3.89	1.125	Agree
41	Lack of effective communication in the family encourages youths involvement in cybercrime activities	3.74	1.142	Agree
42	Parents and guardians ca transmit crime values to their wards	3.97	1.003	Agree
43	Most parents and guardians encourage cybercrime activities	3.53	1.251	Agree
44	Youths from illiterate parents are more prone to criminal activities	3.21	1.273	Agree

The result from Table 14 showed that with an average mean of 3.73, the respondents agreed to all the six items as regards relationship between

family and parents socio-economic background and youth involvement in cybercrimes. The relative low values of the standard deviation show that their responses do not deviate significantly from each other.

Research Question 9: Is there any relationship between education and cybercrime activities among youths in Nigeria?

Table 15: Mean and Standard Deviation of responses on Education and Cybercrimes

S/N	Item Statements	Mean	Std. Dev.	Remark
45	Literate youths are more purposeful in pursuance of positive goals than illiterate ones	3.75	1.164	Agree
46	Uneducated youths are easily influenced by social vices in their societies	3.81	1.069	Agree
47	Education shapes the character and attitude of youths positively	4.14	1.009	Agree
48	Cybercrime and its related activities discourage youths pursuit for academic excellence	3.68	0.900	Agree
49	Media influence such as radio, television, newspaper, and so on	3.68	1.181	Agree
50	Illiterate youths with low educational background are easily influenced towards negative tendencies	3.87	1.053	Agree

The data in Table 15 revealed that the mean values ranged from 3.68 to 4.19, while the standard deviation values ranged from 0.900 to 1.181. With an average mean of 3.91, the result indicates that respondents agreed to all six items as regards relationship between education and cybercrime activities among youths. Meanwhile, the relative low values of the standard

deviation show that their responses do not deviate significantly from each other.

Hypotheses Testing

In the study, six hypotheses were formulated and tested. These include: peer group influence and youth involvement in cybercrime activities; knowledge of the internet and youths' involvement in cybercrime activities; youths' socio-economic status and their involvement in cybercrime activities, gender and participation of youths in cybercrime activities; parents' socio-economic status and youths' involvement in cybercrime activities, and education and cybercrime activities among youths. A summary of the hypotheses tested is presented in Tables 16-21.

Hypothesis 1: There is no significant relationship between peer group influence and youths' involvement in cybercrime activities

The hypothesis was tested using chi-square statistics of peer group influence and youths' involvement in cybercrimes and the result of the analysis is presented in Table 16.

Table 16: Chi-Square Statistics on Peer Influence on Youths' Involvement in Cybercrime

S/N	Item Statements	SA	A	U	D	SD	X^2	df	Sig.	Decision
1	sociological influence can encourage youths involvements in cybercrime	162	199	31	10	6				
2	Youths who are not under direct control or surveillance of their parents are more prone to participation in cybercrime activities	121	166	33	62	26				
3	Criminal behaviours are learned and not inherited	183	172	34	14	5	177.86	4	0.00	H_o is rejected
4	The principal part of learning criminal behaviour occur within intimate personal groups	179	183	29	11	6				
5	Lack of self-control is a driving force behind youths participation in cybercrime activities	159	189	27	23	10				
6	Association with cyber criminals can influence youths involvement in cybercrime activities	196	178	22	10	2				

The data on Table 10 showed a chi-square (X^2) value = 177.86, df=4 and a p-value = 0.00. Testing at an alpha level of 0.05, the p-value is less than 0.05, thus, the null hypothesis which states that there is no significant relationship between peer group influence and youths' involvement in cybercrime activities is rejected. This meant that there is a significant relationship between peer group influence and youths' involvement in cybercrime activities.

Hypothesis 2: There is no significant relationship between the knowledge of the internet and youths' involvement in cybercrime activities

Table 17: Chi-square Statistics on Knowledge of Internet and Youths' Involvement in Cybercrimes

S/N	Item Statements	SA	A	U	D	SD	X^2	df	Sig.	Decision
7	There is a direct link between the knowledge of the internet and cybercrime activities	117	179	56	38	18				
8	Most youths involve in cybercrime because they feel that the internet is a safe place for criminal activities	97	175	64	53	19				
9	Overuse of the internet harms youth academic and social activities	156	164	28	46	14	129.26	4	0.00	Ho is rejected
10	Environment and locality influences youths involvements in cybercrime activities	137	216	25	23	7				
11	Cybercriminals are mainly from the urban areas or centres	89	165	58	67	29				

The data on Table 17 shows a chi-square (X^2) value = 129.26, df = 4 and p-value = 0.00. Testing at an alpha level of 0.05, the p-value is less than alpha level, so, the null hypothesis is rejected. Thus, there is a significant relationship between knowledge of internet and youths' involvement in cybercrime activities.

Hypothesis 3: There is no significant relationship between youths' socio-economic status and their involvement in cybercrime activities.

Table 18: Chi-square Statistics on Youths' Socio-economic Status and Involvement in Cybercrime Activities

S/N	Item Statements	SA	A	U	D	SD	X^2	df	Sig.	Decision
12	Socio-economic factors influences youth participation in cybercrime activities	159	190	28	26	5				
13	Striving for social status is one reason youths participate in cybercrime activities	175	191	16	24	2				
14	Illiterate youths with low educational background are easily influenced towards negative tendencies	143	180	35	39	11	186.29	4	0.00	Ho is rejected
15	Occupational background can influence youths participation in cybercrime	93	181	62	54	18				
16	Youths who are not gainfully employed participate more in cybercrime activities	135	185	30	42	16				

The data on Table 18 showed chi-square (X^2) = 186.29, df=4 and p-value = 0.00. Testing at an alpha level of 0.05, the p-value is less than the alpha level, so, the null hypothesis is rejected. Therefore, there is a significant relationship between youths' socio-economic status and their involvement in cybercrime activities.

Hypothesis 4: There is no significant difference between gender and participation of youths in cybercrime activities.

The hypothesis was tested using the t-test of independent samples of gender on youths' participation in cybercrime activities and the result of the analysis was presented on Table 19.

Table 19: T-test Statistics of Gender on Youths' Participation in Cybercrime Activities

Gender	N	Mean	SD	Mean Difference	df	t	Sig. (2-tailed)	Decision)
Male	207	16.79	3.74	-.910	406	-2.389	.017	H_o is rejected
Female	201	17.90	3.95					
Total	408							

The data on Table 19 shows a t-value of -2.574, df=406, and a p-value of .010 testing at a alpha level of .05. The p-value is less than .05, so, the null hypothesis is rejected. This meant that there is a significant difference between gender and youth participation in cybercrime activities.

Hypothesis 5: There is no significant relationship between parents' socio-economic status and youths' involvement in cybercrime activities.

Table 20: Chi-Square Statistics on Parents' Socio-economic Status and Youths' Involvement in Cybercrime Activities

S/N	Item Statements	SA	A	U	D	SD	X^2	df	Sig.	Decision
17	Parents socio-economic background can influence youths participation in cybercrime activities	130	200	38	32	8				
18	Youths from poor family background are more prone to cybercrime activities because they lack finance for their basic needs	142	160	37	56	13				
19	Lack of effective communication in the family encourages youths involvements in cybercrime activities	107	182	48	47	24	67.83	4	0.00	H_o is rejected
20	Parents and guardian can transmit crime values to their wards	128	197	40	29	14				
21	Most parents and guardian encourage cybercrime activities	100	151	57	64	36				
22	Youths from illiterate parents are more prone to criminal activities	67	137	61	100	43				

The data on Table 20 revealed chi-square (X^2) = 67.83 df=4 and p-value =0.00. Testing at an alpha level of 0.05, the p-value is less than the

alpha level, so, the null hypothesis is rejected. Thus, there is a significant relationship between parents' socio-economic status and youths' involvement in cybercrime activities.

Hypothesis 6: There is no significant relationship between education and cybercrime activities among youths in Nigeria.

Table 21: Chi-Square Statistics on Education and Cybercrime Activities among Youths

S/N	Item Statements	SA	A	U	D	SD	X^2	df	Sig.	Decision
23	Literate youth are more purposeful in pursuance of positive goals than illiterate youths	123	152	61	51	21				
24	Uneducated youths are easily influence by the social vices in their societies	113	179	54	49	13				
25	Education shapes the character and attitude of youth positively	179	160	29	29	11	128.94	4	0.00	H_o is rejected
26	Cybercrime and its related activities discourages youths pursuit for academic excellence	173	175	31	24	5				
27	Media influence such as radio, television, newspaper, etc plays a relative important role in the genesis of criminal behaviour	112	154	65	52	25				
28	Illiterate youths with low educational background are easily influenced towards negative tendencies	119	186	51	36	16				

The data in Table 21 showed chi-square (X^2) = 128.94, df=4 and p-value = 0.00. Testing at an alpha level of 0.05, the p-value is less than the alpha level, so, the null hypothesis is rejected. Therefore, there is a significant relationship between education and cybercrime activities among youths.

Discussion of Findings

The findings on the causes of the misuse of modern technology for cybercrimes by youths showed that they cover unemployment, the quest for

more money, poverty, societal acceptance and parental conflict. This finding can be related to researches that show the causes of cybercrime to include materialistic orientation, effect of globalization, increasing alienation of children, general erosion of values, role of technology (Odey, 2019), influence of the media, vulnerability of adolescents, reluctance to lodge complaints about cybercrime, quest for wealth, weak implementation of cybercrime laws and inadequate equipped law agencies (Laura, 2012), negative role models (Meke, 2012), and so on.

Findings on effect of misuse of modern technology for cybercrime on individuals and society showed that it has a negative effect on society most especially youths' academic achievement, their interpersonal relationship as well as social behaviour. Researches have shown that one major and a common effect of cybercrime activities among Nigerian youths was arrest and in some cases imprisonment (Omojiyugbe & Oyekola, 2019; Babalola, 2019; Ovie, 2019; Odunsi, 2019; & Ogunyinka, 2019. Other researchers, practitioners and policy makers call for the imposition of concrete and efficient mechanisms to control the use of modern technologies to reduce their negative effects on youths (Johnson et al, 2014; Blinka & Smahel, 2006; cupta & Parvesh, 2014).

The findings on non-prosecution of cybercriminals by government and law enforcement agents encouraging youth participation in cybercrimes was in the affirmative. This aligns with the findings of researchers such as Bautray and Toker (2015, Passey et al (2014), Al-Zahrani (2015) and Mareschal et al (2019) who called for efficient and strict legal actions against youths found guilty for practising and engaging in such demeaning activities.

Findings on the relationship between peer group influence and youth involvement in cybercrime showed that peer association could influence youths' cybercrime involvement. In relation to this finding, Baker and Bidin (2014) emphasized that easy access to modern technologies has resulted in many socio-cultural changes especially among young people. Technology changes the way youths interact and communicate with each other, which easily influences their way of life. While the positive sides of modern technologies could be the motives in obtaining and facilitating such technologies to youth, past studies have warned that the negative sides of modern technologies could be harmful to one's social behaviour.

The findings on relationship between knowledge of the internet and cybercrime activities among youths showed that there is a connection between knowledge of internet and cybercrime. This follows the findings of

Baker and Bidin (2014) who stated that youths of different skills, backgrounds and educational levels develop different capacities dealing with technology in a new world. Some youths due to their knowledge of internet get involved in cybercrimes because they feel the internet is safe for criminal activities. Consequent upon this, Longe et al (2018) claimed that a majority of youths are involved in various cybercrimes including e-mail scam, cyber bullying and intimidations, website hacking, internet pornography, child and drug trafficking, pranksters, piracy, examination fraud, financial fraud and sabotaging internet network providers.

The finding on the relationship between Nigerian youths' socio-economic status and their involvement in cybercrime activities showed that a significant relationship exists. In line with this, Nigeria today has young people who engage in this form of anti-social behaviour for the purpose of living a life of splendor. There is the need for the Nigeria government to do something urgent to curb this menace of cybercrime. Several studies have been conducted on the establishment of linkages among the human environment, increasing nature of technological driven business transactions, the growth of fraud and the attendant skepticism revolving around the security of online interaction globally. In one of such studies, Kovacich (2018) reveals that trade on a global scale has been increasing for centuries,

and it is expected to continue to increase, in some areas expanding exponentially and more rapidly than in the past.

The findings on the significant difference in gender and youths' participation in cybercrime activities revealed that there was a significant difference. This is corroborated by Bachmann (2010), Chamtter (1995) and Turgeman-Goldchmidt (2005) who stated that only a few cybercrimes are committed by females, as it appears that cybercrime is predominantly conducted by males. Also, Taylor (1999) stated that the gender ratio at hacking conferences is approximately one female to every one hundred males and that females are often transiently involved in the hacker subculture. Consequently, Hollinger (1993) in his study of one hundred college students found that 5.2 percent of males and 1.8 percent of females admitted to having accessed another's computer account or files without permission.

Findings on the relationship between family and parents' socio-economic background and youth involvement in cybercrimes showed that there is an association between both variables. This finding is in consonance with that of Egbe-Okpenge and Awopetu (2013) who posited that though modern technologies advance education, economy and society, care must be taken when providing and investigating in such technologies both at

individuals and the national levels. They emphasize that parents, school guidance, counsellors and professionals outside the school need to play their roles in directing and protecting youths against the negative consequences of modern technologies that may cause problems to the society.

A cursory look at the findings on the relationship between education and cybercrime activities among youths showed that a link exist between the two. In line with this, the available case studies in Nigeria investigate the positive effects of technology on youths. Thus, Yusop and Sumari (2016) examined the role of technology in assisting students in achieving their academic goals. They found that students are actively engaged in social media sites for information sharing and educational purposes.

Based on the overall findings, it can be said that the causes of cybercrimes among youths which includes unemployment, quest for more money, poverty, societal acceptance as well as parental conflict can have a negative effect on society. Sequel to this, the case of non-prosecution of cybercriminals by government seems to encourage youth participation in the negative activity. Thus, there is the need for appropriate steps to be put in place so as to help in stemming the tide of cybercrimes among youths.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary

This study was carried out to investigate cybercrime and the misuse of modern technologies by youths in the University of Benin, Benin City. Related literature was reviewed to gather information for the study. Nine research questions were raised of which six (6) were hypothesized and tested at 0.05 alpha level of significance. The descriptive survey research design was adopted in this study. The population of the study consisted of 43,772 students (having 39,243 undergraduates and 4.529 postgraduates). A sample of 408 students from five (5) faculties was purposive sampled for the study. A self-designed questionnaire titled "Misuse of Modern Technologies for Cybercrime by Youths (MMTCYQ) was used for data collection. While a descriptive statistics using frequency and percentage was used in analyzing the respondents' demographic data, mean and standard deviation was used in the data analysis of the research questions, while chi-square and t-test of independent samples were used in testing the hypotheses.

The findings based on the research questions raised and hypotheses tested showed the following: unemployment, greed for money, poverty and parental conflict are amongst the leading causes of misuse of modern

technology for cybercrime; cybercrime activities can impact negatively on youths in the areas of academics, interpersonal relationships, social behaviour, and so on; non-prosecution of cybercriminals by government and law enforcement agents encourages youths' participation in cybercrime activities; peer group can encourage youths' involvement in cybercrime activities; there is a direct link between knowledge of internet and cybercrime activities; there exists relationship between socio-economic status of youths and their involvement in cybercrime; males are more inclined to cybercrime and deviant behaviours than their female counterparts; family and parents' socio-economic background is linked to youth involvement in cybercrimes; there is a relationship between education and cybercrime activities among youths.

Conclusion

Based on the findings of the study, it is therefore concluded that the factors that are responsible for youths' engagement in cybercrime should be curbed and/or reduced to the barest minimum, and youths should be encouraged on the need to uphold societal values and shun criminal activities.

Recommendations

In line with the submission above, the following recommendations were put forth:

- The government should formulate workable policies against cybercrime and the misuse of modern technology.
- Children and youths should be taught the dangers of cybercrime activities and they should be educated on the need to open up if they are experiencing any kind of online harassment, stalking or bullying.
- Keeping up to date on major security breaches can be of great advantage.
- Measures should be taken towards protection against identity theft. A Virtual Private Network (VPN) can help to protect the data sent or received online.
- Any victim of cybercrime should be reported to the police, in some cases the Federal Bureau of Investigation (FBI) and Federal Trade Commission.
- Reorientation of values directed at the youths is quite necessary in curbing the menace of cybercrime that is becoming rife among the youths.

- Building confidence among youths can be a component for discouraging participation in cybercrime.
- The challenges of mal-governance, citizens' plight insensitivity, policy failures uncoordinated programmes and several other issues fanning insecurity, hopelessness and crime must be checked to pave way to development in Nigeria.

Contribution to Knowledge

Few studies have been done on the misuse of modern technologies for cybercrime by youths especially using university students as case study. This study has established the causes of the misuse of modern technologies for cybercrime by youths in Nigeria thereby filling the gap between the misuse of modern technologies and cybercrime among university students.

Also, the study has contributed to existing knowledge in the area of the relationship between socio-economic status of youths and their involvement in cybercrime as significant relationship do exist as revealed from the study.

The study will be useful to families who are most of the time victims of cybercrime on how to monitor and educate their children on the negative implications of the involvement in cybercrime activities.

Furthermore, the findings from this study would help the society to know the causes and factors that influences youths' involvement in cybercrime in Nigeria.

Suggestion for Further Studies

Areas for further research on the topic include the following:

1. Sociological implication of youths' involvement in cybercrime activities in Edo State of Nigeria.
2. Modern Technologies as correlate of university student involvement in cybercrime in Nigeria.
3. The Influence of University student involvement in cybercrime on their academic performance.

REFERENCES

Agnew, R. (2000). "Sources of criminality: Strain and subcultural theories". In Joseph F. Sheley (ed), *Criminology: A Contemporary Handbook, 3rd edition, pp.* 349-371. Balmont, CA: Wadsworth.

Ajayi, J. (2006). The making of new Nigeria: The pragmatic roles of the NYSC scheme and Nigeria youth. Nigeria: Mollify Printers.

Ajzen, I. (2005). The theory of planned behaviour. *Organizational Behaviour and Human Decision Process,* 50, 179-211.

Akano, T. (2013). Cybercrime: Nigeria redeems image. The Punch. http://www.punchng.com/business/technology/cyber-crme-nigeria-moves-to-redeem-image. Retrieved on 10th January, 2013.

Akers, R.L. & Christine, S.S. (2004). Criminological theories: Introduction and evaluation, 4th edition. Los Angeles: Roxbury Publishing.

Akers, R.L. (1998). Social learning and social structure: A general theory of crime and deviance. Boston: Northeastern University Press.

Akers, R.L. (1998). Social learning and social structure: A general theory of crime and deviance. Boston: Northeastern University Press.

Akers, R.L. & Lee, G. (1996). A longitudinal test of social learning theory: Adolescent smoking. *Journal of Drug Issues,* 26:317-343.

Akinsehinde, G. (2011). Why hackers become crackers – Analysis of conflicts faced by hackers. *Public Administration Research,* 5(10.

Albrecht, S.W.; Albrecht, C.O.; Albrecht, C.C. & Zimbelman, M.F. (2012). Fraud examination. Fourth edition. South-Western: Cengage Learning.

Al-Zahrani, A.M. (2015). Cyberbullying among Saudi's Higher-Education students: Implications for educators and policymakers. *World Journal of Education,* 5(3), 15-26.

Bachmann, M. (2010). "The risk propensity and rationality of computer hackers". *International Journal of Cyber Criminology,* 4: 643-656.

Bakar, S.A. & Bidin, R. (2014). Technology acceptance and purchase intention towards movie mobile advertising among youth in Malaysia. *Procedia-Social and Behaviour Sciences,* 1(3), 558-567.

Bandura, A. (1977). Social learning theory. Oxford England: Prentice Hall.

Banerveldr, C.; Knecht, A.; Raub, W.; Snijders, T.A.B. & Steglich, C.E.G. (2010). Friendship and delinquency: Selection and influence processes in early adolescence. *Social Development,* 19(3): 494-514.

Baudrillard, J. (1984). Simulations. New York: Semiotex(e).

Bautray, M.H. & Toker, S. (2015). An investigation of the impact of demographics on cyberloafing from an educational setting angle. *Computers in Human Behaviour,* 50, 358-366.

Beccaria, C. (1983). An essay on crimes and punishment. Brookline Village, MA: Branden Press.

Becker, H. (1963). Outsiders: Studies in the sociology of deviance. New York: The Free Press.

Benson, M. & Moore, E. (1992). "Are white-collar and common offenders the same?". *Journal of Research in Crime and Delinquency,* 29:251-272.

Blinka, L. & Smahel, D. (2016). Predictors of adolescents' excessive internet use: A comparison across European countries. *Proceedings of the 15th European Conference on development Psychology* (pp. 337-342). Bolognu, Italy, Mediamond.

Bottcher, J. (2001). "Social practices of gender: How gender relates to delinquency in the everyday lives of high-risk youths". *Criminology,* 39: 893-931.

Brette, O. (2003). "Thorstein Veblen's theory of institutional change: Beyond technological determinism". *European Journal of the History of Economic Thought.* 10(3), 455-477.

Castells, M. & Pekka, H. (2002). *The Information Society and the Welfare State: The Finish Model.* Pg. 208-23, Oxford Up, Oxford.

Cha, A. (2005). Police find that on Ebay some items are a real steal. Retrieved 8 January, 2017. http://www.duluthsuperior.com/mid/duluthsuperior/ 10597328.htm.

Chantler, A.N. (1995). "Risk: The profile of the computer hacker". Unpublished thesis. Curtin University.

Clausen, L. (1991). "Gemeinschaft and Gesellschaft". Opladen: Leske Budrich, Germany.

Comte, A. (1865). A general view of positivism. Cambridge: Trubner and Co.

Crozier, B. (1974). A theory of conflict. London: Hamish Macmillan.

Currie, E. (1985). Confronting crime: An American challenges. New York: Pantheon.

Daly, K. (1992). Women's pathways to felony court: Feminist theories of lawbreaking and problems of representation. *Southern California Review of Law and Social Justice,* 2:11-52.

Denning, D.E.R. (1999). *Information Warfare and Security,* Pg. 166, Addison Wesley, Indian Reprint.

Dunn, W. & Wigert, I. (2004). Critical infrastructure (CI) is defined as `an infrastructure or asset, the incapacitation or destruction of which would have a debilitating impact on the national security or economic or social welfare of a nation. *International CIIP Handbook: An Inventory and Analysis of Protection Policies in Fourteen Countries.* Pg. 18, Swiss Federal Institute of Technology, Zurich.

Durkheim, E. (1893/1933). The division of labour in society. New York: The Free Press.

Dutton, G. & Helsper, S. (2009). Fraud masters: Professional credit card offenders and crime. *Criminal Justice Review,* 19 (Spring), 24-55.

Einstadter, W. & Stuart, H. (1995). Criminological theory. Fort Worth, Tx: Harcourt Brace.

Evans, T.D.; Francis, T.C.; Velmer, S.B.; Gregory, R.D. & Michael, L.B. (1997). "The social consequences of self-control: Testing the general theory of crime". *Criminology,* 35: 475-504.

Ewepu, G. (2016). Nigeria loses N127bn annually to cybercrime NSA, http://www.vanguardngr.com/2016/04. Retrieved January 9, 2016.

Farrington, D.P. (2002). Risk factors for youth violence (pp. 25-57). Brasilia: Unesco.

Francoi, S.L. (2003). Social psychology. New York: McGraw-Hill Companies Inc.

Fischer, (2007). DicZeit04.01.2017, http://newsbbc.co.uk/english/ static/indepth/ uk.2001/lifeofcrime/cybercrimes. Retrieved February 12, 2019.

Flemming, P. & Stohl, M. (2000). Myths and realities of cyberterrorism. *International Conference on Countering Terrorism through Enhanced International Cooperation,* 22-24.

Francis, T.C. & Pamela (2010). Wilcox encyclopedia of criminological theory. New York: Sage Publications.

Gelsthorpe, L. & Wright, S. (2015). The context: Women as lawbreakers. In J. Annison, J. Brayford and Deering (eds). Women and criminal justice: From the Corston Report to Transforming rehabilitation. Bristol: Policy Press.

Gibson, W. (1984), Neuromancer, Pg. 4, Ace Hardcover, New York.

Giddens, A. (1991). Modernity and self-identity. Self and society in the late modern age. Pg. 214. Cambridge: Polity Press.

Google.com/amp/s/punchng.com/EFCC.

Gottfredson, M.R. & Hirschi, T. (1990). A general theory of crime. CA: Stanford: Stanford University Press.

Gottfredson, M.R. & Travis, H. (1990). A general theory of crime. Stanford, CA: Stanford University Press.

Gottfredson, M.R. (2006). "The empirical status of control theory in criminology". In Francis T. Cullen, John Paul Wright and Kristie R. Blevins (eds). *Taking Stock: The Status of Criminology Theory - Advances in Criminological Theory.*

Gottfredson, M.R. (2006). "The empirical status of control theory in criminology". In Francis T. Cullen, John Paul Wright, and Kristie R. Blevins (eds). *Taking Stock: The Status of Criminology Theory – Advances in Criminological,* 15: 77-100.

Grasmick, H.G.; Charles, R.T.; Robert, J.B.J. & Bruce, K.A. (1993). "Testing the core empirical implications of Gottfredson and Hirschi's implications of crime". *Journal of Research in Crime and Delinquency,* 30: 5-29.

Gupta, M. & Laga, P. (2014). Absenteeism in schools: A chronic problem in the present time. *Educ. Confab.* 3(1), 11-16.

Haynie, D.L. & Osgood, D.W. (2005). Reconsidering peers and delinquency: How do peers matter social force, 84(2), 1109-1130.

Heimer, K. & De Coster, S. (1999). The gendering of violent delinquency. *Criminology,* 37: 277-318.

Hirschi, T. (1969). Causes of delinquency. Berkeley and Los Angeles: California Press.

https://dailypost.ng.metro.

https://google.com/amp/s/dailypost.ng/2019/08/07.

https://google.com/amp/s/punchng.com.

https://www.ecrimeresearch.og.

https://www.Saharareporters.com/2019/08/08dessarrests.

https://www.vanguardngr.com.

https://www/pulse.ng.local.

Igbo, H.I.; Egbe-Okpenga, E.G. & Awopetu, R.G. (2013). Influence of Information and Communication Technology on behavour problems of Nigeria youths. *Procedia-social and Behavioural Sciences,* 84:97-106.

India Digital Future in Focus (2013). Retrieved from www.comscore.com/ content/india-digital-futrue-in-focus.2013.

Jaishankr, K. (2007). Establishing a theory of cybercrime. *International Journal of Cyber Criminology.* 1(2), 7-9.

Jameson, F. (1991). Postmodernism or the cultural logic of late capitalism. Durham, NC: Duke University Press.

Jegede, A.E.; Olomookere, E.I. & Elegbeleye, A.O. (2016). Youth identify, peer influence and internet crime participation in Nigeria: A reflection. *Ife Psychology IA,* 24(1), 37-47).

Jenkins, R. (2008). Social identity (3rd ed.). New York: Routledge.

Jonsson, L.S.; Priebe, G.; Bladh, M. & Svedin, C.G. (2014). Voluntary sexual exposure online among Swedish youth-social background, internet behavhiour and psychosocial health. *Computers in Human Behaviour,* 30, 181-190.

Jordan, T. & Taylor, P. (1998). A sociology of hackers. *The Sociological Review,* 46: 757-780.

Kovacich, G.L. (2018). Fighting fraud: How to establish and manage anti-fraud program. UK: Elsevier Academic Press.

Kshetri, N. (2010). *The Global Cybercrime Industry.* New York: Springer, p. 3.

Lane, F. (2001), Lone has *Obscene profits: The Entrepreneurs of Pormography in the Cyber Age,* pg. 66. London: Routledge.

Latane, B. (1981). The psychology of social impact. *American Psychologist,* 36, 343-356.

Lemo, M. (2013). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behaviour,* 34, 165-172.

Longe, O.; Ngwa, F.; Wada, F. & Mbarika, V. (2018). Criminal uses of ICT in Sub-sahara Africa: Trends , concerns and perspectives. *Journal of Information Impact,* 9(3), 155-172.

Marcus, R.F. (1996). The friendships of delinquents. *Adolescence,* 31(121): 145-158.

Mareschal, P.M.; McKee, W.L.; Jackson, S.E. & Hanson, K.L. (2017). Technology-based approaches to preventing youth violence a formative evaluation of program development and implementation in four communities. *Youth Violence and Juvenile Justice,* 5(2), 168-187.

Martin, R.; Robert, J. & Timothy, W.A. (1990). Criminological thought: Pioneers past and present. New York: Macmillan.

Matsueda, R.L. (1988). "The current state of differential association theory". *Crime and Delinquency,* 34: 277-306.

Merton, R.K. (1938). Social structure and anomie. *American Sociological Review,* (3)672-682.

Mill, J.S. (1859). "Indianapolis: Library of Liberal Arts.

Mulligan, M. (1932). Marx economic and philosophic manuscripts of 1844 (Translated), Moscow: Progress Publishers.

Network Society (1996). The term network society was coined in Norwegian by Stein Braten in his book in his book Modeller av menneske og samfunn (1981). Later the term was put to use in Dutch by Jan van Dijk

in his book De Networkmaatschappij (1991) (The Network Society) and by Manual Castells in The Rise of the Network Society.

Nigerian Institute of Social and Economic Research (NISER) (2003). Understanding poverty in Nigeria. *NISER Review of Economic Development 2001/2002.* Ibadan, Nigeria: College Press and Publishers Ltd.

Ozughalu, U.M. (2008). Poverty, underdevelopment and global competitiveness: A reflection on Nigeria's situation, NSEG. *Economic Indicators,* 14(3), 48-52.

Parsons, T. (1961). Theories of society: Foundations of modern sociological theory. The Free Press of Glencoe, Illinios. Pg. 1061-1062.

Passey, D.; Rogers, C.; Machell, J. & McHugh, G. (2014). The motivational effect of ICT on pupils. Research Report 523. Department of Educational Research Lancaster University. Accessed on 18 August, 2015 via http://downloards01.smarttech.com/media/research/international_research/uk/lancaster_reprot.pdf.

Pfohl, S.J. (1985). Images of deviance and social control. New York: McGraw-Hill.

Pratt, T.C. & Francis, T.C. (2000). "The empirical status of Gottfredson and Hirshi's general theory of crime: a meta-analysis". *Criminology* 38: 931-964.

Ritzer, G. (2008). The McDonalization of society. Pp. 351-384. Los Angeles: Pine Forge Press.

Ritzer, G. (2011). Sociological theory. New Delhi: Tata McGraw Edition.

Royal Canadian Mounted Police, (2010). European treaty series – No 185, council of Europe, cybercrime… and punishment? Archaic laws threaten global information". A report prepared by McConnell International "Cybercrime", Mingail S., Canada Law Book Inc. 2003, http://www.canadalawbook. ca/headlines/headlines317_arc.html.

Schwartz, J.; Steffensmeier, D.; Zhong, H. & Ackerman, J. (2009). Trends in the gender gap in violence: Reevaluating NCVS and other evidence. *Criminology,* 47:401-425.

Seller, C.S. (1999). "Self-control and intimate violence: An examination of the scope and specification of the general theory of crime". *Criminology,* 37: 375-404.

Sesay, A.; Ukeje, C.; Aina, O. & Odebiyi, A. (2003). Ethnic militia and future of democracy in Nigeria. Ile-Ife: Obafemi Awolowo University Press.

Shade, L.R. & Shepherd, T. (2013). Viewing youth and mobile privacy through a digital policy literacy framework. First Monday, 1g (rz), <http:ilfirestmonday.org/ojs/index.phpIfm/article1view/4g07?;viewed,zl. 0z.15.

Skinner, W.F. & Fream, A.M. (1927). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency,* 34:495-518.

Steffensmeier, D. & Allen, E. (1996). Gender and crime: Toward a gendered theory of female offending. *Annual Review of Sociology,* 22:459-487.

Sutherland, E.H. (1924). Principles of criminology. Chicago: University of Chicago Press.

Tade, O. & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology,* 5(2), 860-875.

Tarde, G. (1903). The laws of imitation. New York: H. Holt and Company.

Taylor, P.A. (1999). Hacker. London: Routledge.

The Star Online (2014). Malaysia is sixth most vulnerable to cybercrime. http://www.thestar.com.my/news/national20t41091231cyber-crime-malaysianssixth-most-vulnerable.

Thomas, D. & Loader, B. (2000), Cybercrime law enforcement, security and surveillance in the information age. London: Routledge, p. 8.

Thomas, J.; Holt, Adam, M.B. & David, C.N. (2011). Low self-control, deviant peers associations and juvenile cyber deviance, 3-5.

Turgeman-Goldschmidt, O. (2005). Hackers' account hacking as a social entertainment. *Social Science Computer Review,* 23: 8-23.

Ulrich, B. (1992). Risk Society: Towards a new modernity. New Delhi: Sage.

Unnever, J.D.; Francis, T.C. & Robert, A. (2006). "Why is `bad' parenting criminology? Implications from rival theories". *Youth Violence and Juvenile Justice,* 4:3-33.

Vold, G.B.; Thomas, J.B. & Jeffrey, B.N. (2002). Theoretical criminology. New York: Oxford University Press.

Warr, M. (2001). "The social origins of crime: Edwin Sutherland and the theory of differential association". In Raymond Paternoster and Ronet Bachman (ed.),. *Explaining Criminals and Crime,* pp. 182-191. Los Angeles: Roxbury Publishing.

Weber, M. (1991). The nature of social action in Runciman, W.G. Weber: Selection in translation. UK, Cambridge: University Press.

Wells, L.E. & Joseph, H.R. (1988). "Direct parental controls and delinquency". *Criminology,* 26:263-285.

Young, K. (1998). Internet addiction: The emergence of a new clinical disorder. *Cyber Psychology and Behaviour*, 1(3), 237-244.

Yusop, F.D. & Sumari, M. (2013). The use of social media technologies among Malaysian youth. In International educational technology conference (IETC), Kuala Lumpur, Malaysia.

Zimmer, E. & Hunter, D. (1999). Risk and the Internet Perception and Reality. Retrieved from www.copacommission.org/papers/webriskanalysis.pdf.

APPENDICES

APPENDIX I

DEPARTMENT OF EDUCATIONAL FOUNDATIONS
FACULTY OF EDUCATION
UNIVERSITY OF BENIN

MISUSE OF MODERN TECHNOLOGIES FOR CYBERCRIME BY YOUTHS QUESTIONNIARE (MMTCYQ)

Dear Respondents,

The researcher is a postgraduate student in the Department of Educational Foundations, Faculty of Education, University of Benin, carrying out an academic study titled "The Misuse of Modern Technologies for Cyber Crime by Youths: The Nigerian Experience".

Please, respond appropriately and honestly to the questions below by ticking (√) the option that appeals most to you. Information from responses for this study would only be used for academic purposes and therefore treated with utmost confidentiality.

Thank you.

Yours faithfully,

ThankGod Onyebuchi IBE

Section A: Biodata

Gender: Male ( ) Female ( )

Age of Respondent: Below 18yrs ( ) 18-20yrs ( ) 21-24yrs ( ) 25-30yrs ( ) 31-35yrs ( ) 35yrs and above ( )

Location of Respondent: Urban ( ) Rural ( )

Faculty:_____

Department:_____

Academic Level: 400 ( ) Masters ( )

Section B

Key:

SA = Strongly Agreed

A = Agreed

U = Undecided

D = Disagree

SD = Strongly Disagree

S/N	Items	SA	A	U	D	SD
	Causes of Cybercrime					
1	Unemployment is a motivating factor for the involvement of youths in cybercrime activities					
2	Youths participation in cybercrime majorly to get more money					
3	Poverty is a major factor for the involvement of youths in cybercrime					
4	The Nigerian youths appreciates cybercrime as an opportunity for wealth and affluence					
5	The contemporary Nigerian society appreciates and applaud dividends from cybercrimes and cybercriminals					
6	Parental conflict can be responsible for the involvement of youths in cyber related crimes					
	Effects of Cybercrime and the Misuse of Modern Technologies					
7	Cybercrime has negative effect on the Nigeria society					
8	The misuse of modern technologies by youths has a positive effect on them					
9	Cyber-crime is a legal method for wealth creation					
10	Involvement in cybercrime activities can affect youths academic pursuit and achievements					
11	Cybercrime activities influences youths interpersonal relationship negatively					
12	Cybercrime activities affects social behaviour among Nigerian youths					
	Peer Group Influence on Cybercrime Activities in Nigeria					
13	sociological influence can encourage youths involvements in cybercrime					
14	Youths who are not under direct control or surveillance of their parents are more prone to participation in cybercrime activities					
15	Criminal behaviours are learned and not inherited					

S/N	Items	SA	A	U	D	SD
16	The principal part of learning criminal behaviour occur within intimate personal groups					
17	Lack of self-control is a driving force behind youths participation in cybercrime activities					
18	Association with cyber criminals can influence youths involvement in cybercrime activities					
	Influence of Government and Law Enforcement Agents on Cybercrime Activities					
19	Refusal to lodge complaints about cybercrime to relevant authorities helps to encourage more involvement in cybercrime activities					
20	Instability of government policies encourages youths involvements in cybercrime activities					
21	The law enforcement agents in most cases encourage cybercriminals through lack of proper investigation					
22	Failure to prosecute cybercriminals can encourage more participation in cybercrime activities					
23	The absence of effective punishments on cybercriminals encourages more participation					
	The Use of the Internet and Cybercrime					
24	There is a direct link between the knowledge of the internet and cybercrime activities					
25	Most youths involve in cybercrime because they feel that the internet is a safe place for criminal activities					
26	Overuse of the internet harms youth academic and social activities					
27	Environment and locality influences youths involvements in cybercrime activities					
28	Cybercriminals are mainly from the urban areas or centres					
	Socio-Economic Status of Nigerian Youths and Involvement in Cybercrime					
29	Socio-economic factors influences youth participation in cybercrime activities					
30	Striving for social status is one reason youths participate in cybercrime activities					
31	Illiterate youths with low educational background are easily influenced towards negative tendencies					

S/N	Items	SA	A	U	D	SD
32	Occupational background can influence youths participation in cybercrime					
33	Youths who are not gainfully employed participate more in cybercrime activities					
	Gender and Involvement in Cybercrime					
34	Female cybercriminals are not volatile as their male counterparts					
35	Participation of the males are more prominent than their females counterpart in cybercrime activities					
36	Females participate in cybercrime activities just for fun and entertainment					
37	Gender is a major factor in the participation of cybercrime activities					
38	Deviant behaviours are rampant among males					
	Family and Parents Socio-Economic Background and Youths Involvement in Cybercrime					
39	Parents socio-economic background can influence youths participation in cybercrime activities					
40	Youths from poor family background are more prone to cybercrime activities because they lack finance for their basic needs					
41	Lack of effective communication in the family encourages youths involvements in cybercrime activities					
42	Parents and guardian can transmit crime values to their wards					
43	Most parents and guardian encourage cybercrime activities					
44	Youths from illiterate parents are more prone to criminal activities					
	Education and Cybercrime among Youths					
45	Literate youth are more purposeful in pursuance of positive goals than illiterate youths					
46	Uneducated youths are easily influence by the social vices in their societies					
47	Education shapes the character and attitude of youth positively					
48	Cybercrime and its related activities discourages youths pursuit for academic excellence					
49	Media influence such as radio, television, newspaper, etc plays a relative important role in the genesis of criminal behaviour					
50	Illiterate youths with low educational background are easily influenced towards negative tendencies					