

**PATTERN AND CONSEQUENCES OF CYBER-CRIME IN TERTIARY
INSTITUTIONS IN ZARIA**

By

**Kazeem Abimbola ADETA
(M.SC/SOC-SCI/5795/2009-2010)**

**A THESIS SUBMITTED TO THE SCHOOL OF POSTGRADUATE
STUDIES, AHMADU BELLO UNIVERSITY, ZARIA, IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A
MASTER DEGREE IN SOCIOLOGY.**

**DEPARTMENT OF SOCIOLOGY
FACULTY OF SOCIAL SCIENCES
AHMADU BELLO UNIVERSITY, ZARIA
NIGERIA.**

JUNE, 2014

DECLARATION

I declare that the work in this thesis entitled **Pattern and Consequences of Cyber-Crime in Tertiary Institutions in Zaria** has been carried out by me in the Department of Sociology, under the supervision of Dr J.E. Gyong and Dr B.F. Okeshola. The information derived from the literature has been duly acknowledged in the text and a list of references provided. No part of this thesis was previously presented for another degree or diploma at this or any other Institution.

.....
Kazeem Abimbola ADETA

.....
Date

CERTIFICATION

This thesis entitled **PATTERN AND CONSEQUENCES OF CYBER-CRIME IN TERTIARY INSTITUTIONS IN ZARIA** by KAZEEM ABIMBOLA ADETA meets the regulations governing the award of the degree of Masters of Science in Sociology of the Ahmadu Bello University, Zaria and is approved for its contribution to knowledge and literary presentation.

.....
Dr J.E Gyong Date
Supervisor

.....
Dr B.F Okeshola Date
Supervisor

.....
Dr B.F Okeshola Date
Acting Head of Department

.....
Pro A.A Joshua Date
Dean, School of Postgraduate Studies

DEDICATION

This thesis is whole-heartedly dedicated to Almighty Allah and in memory of my late father Wing Commander I.S Adeta who died on the 22 October 2011. May Allah reward him with Aljana Fridaus (amin).

ACKNOWLEDGEMENTS

All thanks and praise is to Allah, the beneficent and the merciful who protected and guided me throughout this programme.

My special appreciation goes to Dr J.E Gyong and Dr B.F Okeshola who helped bring this project to a successful conclusion. For many months, they were extraordinarily patient in guiding me through the writing process. I will always owe them a professional debt of gratitude. May Allah reward you both.

I will also wish to extend sincere thanks to all lecturers and staffs of the Department of Sociology, A.B.U Zaria for their contribution to the realization of this goal.

My special thanks go to my beloved wife Alhaja Medinat Kemi Adeta for her love and support. I am blessed to have you as a wife and my unquantifiable thanks also go to my mother, Deaconess M.B Adeta for her motherly love.

I wish to acknowledge and thank the following people: my friend Kaseem Zubaru for printing and photocopying my questionnaires, Mr X an operator of cyber-café who got someone who introduced me to a cyber-criminal, all the operators of cyber-café who granted me audience, all the lecturers from the Department of Computer Science in the three selected tertiary institutions in Zaria who participated in the research for their expertise contributions on the subject and the 2 cyber-criminals that participated in the research. Together we have made another important contribution to societal understanding on the subject. I am also grateful to Maryam Adeta for her efforts in working on this project with me.

A big thank you to my friends; Akeem Oloriegbe, Tunde Raheem, Saka Abdulkadri, Abubakar Mohammed Bashir, Afeeze Onabanjo, Captain Kent Samuel and Captain Jude Dimkpa.

TABLE OF CONTENTS

Title Page	i
Declaration	ii
Certification	iii
Dedication	iv
Acknowledgements	v
Table of Contents	vi
List of Tables	ix
List of Figures	x
Abstract	xi

1.0 INTRODUCTION

1.1	Background of the Study	1
1.2	Statement of Problem	4
1.3	Research Questions	7
1.4	Aim and Objectives of the Study	8
1.5	Significance of the Study	8
1.6	Scope of the Study	9
1.7	Definition of Key Terms	10

2.0 REVIEW OF LITERATURE AND THEORETICAL FRAMEWORK

2.1	Introduction	11
2.1.1	Origin of internet	11
2.1.2	Origin and types of cyber-crime	15

2.1.3	Techniques cyber-criminals use to perpetrate cyber-crime	24
2.1.4	Categories of individuals involved in cyber-crime	27
2.1.5	Causes of cyber-crime in Nigeria	30
2.1.6	Consequences of cyber-crime on Nigeria economy	31
2.2	Theoretical Framework	33
3.0	METHODOLOGY	
3.1	Introduction	39
3.2	Location of the Study	39
3.3	Types and Sources of Data	44
3.4	Techniques of Data Collection	45
3.5	Population and Sampling Procedures	46
3.6	Techniques of Data Analysis	51
3.7	Problems Encounter in the Field	52
4.0	ANALYSIS AND INTERPRETATION OF DATA	
4.1	Introduction	53
4.2	Socio-Demographic Characteristic of Respondents	53
4.3	Pattern of Cyber-Crime	54
4.4	Types of Cyber-Crime	64
4.5	Social Attributes of Cyber-Criminals	66
4.6	Causes of Cyber-Crime	75
4.7	Consequences of Cyber-Crime	80
4.8	Solution to Cyber-Crime	82

5.0	SUMMARY, DISCUSSION, CONCLUSION AND RECOMMENDATIONS	
5.1	Introduction	89
5.2	Summary of Major Findings	89
5.3	Discussion of Key Findings	92
5.4	Conclusion	95
5.5	Recommendations	96
	References	98
	Appendix I: Questionnaire for Students of Tertiary Institutions	
	Appendix II: Interview Guide for Cyber-Café Operators	
	Appendix III: Interview Guide for Lecturers of Computer Science Department in Tertiary Institution	
	Appendix IV: Interview Guide for Individuals who indulge in Cyber-Crime	

LIST OF TABLES

Table 4.3.1:	Access to Internet.	54
Table 4.3.2:	Awareness of the Term Cyber-Crime.	56
Table 4.3.3:	Frequency of Cyber-Crime in Tertiary Institutions in Zaria.	57
Table 4.3.4:	Persons Involved in Cyber-Crime.	58
Table 4.3.5:	Time of Perpetration of Cyber-Crime.	59
Table 4.3.6:	Point/Place where Cyber-Crime is Perpetrated.	60
Table 4.3.7:	Nomenclatures of Perpetrators of Cyber-Crime.	61
Table 4.5.1:	Sighting of Cyber-Criminals.	66
Table 4.5.2:	Friends who engage in Cyber-Crime.	68
Table 4.5.3:	Social Attributes of Cyber-Criminals.	69
Table 4.6.1:	Causes of Cyber-Crime.	77
Table 4.8.1:	Respondents views Whether Cyber-Crime can be Controlled.	82
Table 4.8.2:	Solutions to Cyber-Crime.	83

LIST OF FIGURES

Figure 1:	Respondent use of Internet.	55
Figure 2:	Techniques/Tools used by Cyber-criminals.	62
Figure 3:	Types of Cyber-crime.	65
Figure 4:	Life Style of Cyber-criminals.	74
Figure 5:	Consequences of Cyber-crime.	80

ABSTRACT

This research work was conceived to find out the pattern of cyber-crime in tertiary institutions in Zaria, identify the types of cyber-crime common in the study area, explore the social attributes of those involved in cyber-crime in the study area, identify the motivating factor and causes of cyber-crime, find out the consequences of the emerging trends and finally suggest solutions to mitigate against the menace. The study adopted the differential association theory which was developed by Edwin Sutherland to explain the reason for individual's involvement in cyber-crime and how they learnt the techniques to perpetrate the act through interaction with others. The study was conducted in three selected tertiary institutions in Zaria namely; Ahmadu Bello University, Nuhu Bamalli Polytechnic and Federal College of Education. Data was obtained through quantitative method (questionnaires) and qualitative method (In-depth interview). The research also used both probability and non probability sampling method in the selection of respondents. Four hundred questionnaires were administered to students of the three selected tertiary institutions using the simple random sampling method. In addition, 10 key informants were purposively selected for the in-depth interview in order to gain substantial facts on the subject. Snowball sampling method was also used to identify the cyber-criminals who participated in the research. The key informants used for the study are lecturers of computer science department, operators of cyber-café and cyber-criminals. Data collected through quantitative instrument was subjected to simple statistical analysis and interpretation and analyzed with the aid of a computer using the Statistical Package for Social Sciences (SPSS version 17.0). While data collected through the qualitative instrument was transcribed from field notes and tapes. The data collected were presented using tables and bar charts.

The study revealed that youths who are mostly male are the major perpetrator of cyber-crime and the crime can be committed at any time of the day. The research was able to unveil additional techniques such as SQL injection and mathematical model which are used for piracy and credit card fraud respectively by cyber-criminals. Nevertheless, the study found that unemployment, poverty, absence of law and corruption are the major causes of cyber-crime in the study area. Despite the negative consequences of cyber-crime on the study area, it was discovered that it had positive effect for the perpetrators as they were able to use the money realized to solve their need. On the basis of these findings, it was recommended that the Federal Government should empower the youths in terms of job creation and regularly engage the IT industries to develop strategies to curtail cyber-crime. The study also recommends that everybody should report to law enforcement agencies any one suspected to be involved in cyber-crime.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The invention of electronic devices such as modern communication hard-wares, internet service and computer systems has been a major landmark in human history. Ayantokun (2006), defined computer as a machine that performs tasks, such as calculation or electronic communication, under the control of a set of instructions called a program. Programs usually reside within the computer and are retrieved and processed by the computer's electronics. The program results are stored or routed to output devices, such as video display monitors or printers. Oyewole and Obeta (2002), define a computer as an electronic device that accepts, processes, stores and outputs data at high speed according to programmed instructions. Computers perform a wide variety of activities reliably, accurately and quickly depending on the purpose it was designed for. Computer can be used in areas of education, medicine, engineering design, scientific research, office automation, personal administration etc (Morley and Parker, 2007).

According to Rogers (1995), the rapid evolution of the computer brought the internet. The internet services have reduced the world into a global village which makes it look as if everybody is in the same place at a particular point in time. Aside the fact that the internet has made communication to be easier and faster, a lot of other transactions are consummated at the speed of lightening. Oyewole and Obeta (2002), state that the internet is the inter connection of computer across the world thereby creating unlimited opportunities for mankind. Ehimen and Bola (2009), state that cyberspace has provided a save haven for internet platform, which has created geometric growth and accelerated windows of opportunities for businesses and the

removal of economic barriers hitherto faced by nations of the world. People from diverse areas of human endeavor can now freely access and utilize the advantages offered by internet platform. In addition, Young Media Association (2007), listed the following as the positive gain the internet has brought to the world:

- a. Facilitation of job search and employment.
- b. Accessibility to research information for education and businesses.
- c. Rural integration.
- d. Enhancement of trade and commerce.
- e. Sharing of resources and ideas.
- f. Enhance communication.

Considering these limitless advantages of the internet, one can easily subscribe to the fact that it is an important tool for national development in a developing country like Nigeria. However, despite the development trend associated with the internet, it has brought about a new wave of crime which is threatening the social order in the society. The internet online services, which are ordinarily suppose to be blessings as they exposes one to a lot of opportunities in various field of life are fast becoming sources of discomfort and worry due to the atrocity being perpetrated through it. For instance, Salihu (2007), noted that the convergence of computing and communication have brought immense benefits to the society but these benefits also come with greater risk both nationally and internationally. This form of crime is commonly referred to as cyber-crime which is the latest and perhaps the most complicated problem in the cyber world

today. It covers a wide range of illegal activities on the cyber space. Cyber-crime simply means the use of computers and internet as tools to conduct criminal activity such as financial fraud, identity theft, phishing and copyright violations amongst others.

Some individuals in Nigeria have embraced cyber-crime as a way of life. Many have become rich while some others have been caught by the law (Tade and Aliyu, 2011). This new crime is denting and drilling holes in the economy of the nation. For example, in a recent report by the Internet Crime Complaint Center which is a partnership between the FBI and America's National White Collar Crime Center, revealed that Nigeria now ranked third among the list of top ten sources of cybercrime in the world (Abdulhamid *et al*, 2011). Also the Central Bank of Nigeria (CBN) in its banking sector supervision report revealed that the Nigeria banking sector lost 7.2 billion naira to internet fraud (Ajewole, 2010). Losing 7.2 billion naira in a developing economy such as ours is not something to be proud about. Apart from the destruction cyber-crime does to the economy, it also leads to the erosion of confidence in genuine Nigerian commercial credibility and today many western countries with France taking the lead have moved to deny Nigerian businessmen and women who are legitimate the rewards of e-commerce. France today requires web camera verification for most online business transactions from Nigeria (Longe and Chiemeké, 2008).

The youths in every society are of great importance and of great concern to that society because they are looked upon as the leaders of tomorrow. Olaide and Adewole (2004), observed that a sizeable number of criminals in Nigeria fall within the youthful ages and this youthful ages according to them ranged between 18-30 years. The youths at present have discovered different ways of using the internet in doing different types of criminal activities. In furtherance, these age brackets are usually found in tertiary institutions in Nigeria. The word tertiary simply means the third part or rank. Therefore, after the secondary education the next educational level is the

tertiary education which provides advance instructional curriculum to students with a view to develop them for careers in life. Tertiary institutions include universities, polytechnics, colleges of education and colleges of technology. In most Nigeria tertiary institutions, various form of crimes are being witnessed ranging from examination malpractices, falsification of admission, rape, robbery and stealing, sexual abuse, assault, cultism amongst others. But in recent times cyber-crime, a new form of crime, now exists in our tertiary institutions. Students of tertiary institution now engage in cloning of websites, falser representations, internet purchase and other e-commerce kinds of fraud such as credit card fraud (Ribadu, 2007). It is for this reasons, this study work was conceived to study the pattern and consequences of cyber-crime in tertiary institutions in Zaria and suggest solutions to the problem.

1.2 Statement of the Problem

The contribution of internet to the development of the nation has been marred by the evolution of a new wave of crime. The internet has also become an environment where the most lucrative and safest crimes thrive. There are indications that cyber-crime is rising. For example, a 2005 YouGov poll of UK Internet users found that 1 in 20 had lost money in online scams. Also a 2001 survey revealed that 52 per cent of companies interviewed said internet fraud posed real problems for them (Wall, 2007). These are clear indications that cyber-crime is on the increase and as such, it is beginning to gain recognition at the global level and there is dearth of study in the area of this burgeoning criminal act in Nigeria.

Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the

electronic market is opened to everybody (which includes eavesdroppers and criminals), false pretence find a fertile ground in this situation. Vladimir (2005), said the internet is a global network which unites millions of computer located in different countries and open broad opportunities to obtain and exchange information but it is now being used for criminal purposes due to economic factors. Nigeria, a third world country is faced with so many economic challenges such as unemployment amongst others, which are capable of making this crime thrive. Apart from the economy factor been a possible cause of cyber-crime in Nigeria, there might be other causes for the continued rise in cyber-crime activity.

In Nigeria, perpetrators of this crime who are commonly referred to as “yahoo yahoo boys” take advantage of e-commerce system available on the internet to defraud victims who are mostly foreigners thousands and sometimes millions of dollars. They fraudulently represent themselves as having particular goods to sell or that they are involved in a loan scheme project. They may even pose to have financial institution where money can be loaned out to prospective investors. In this regard, persons and organization are duped or have fallen victims. However, these are not the only techniques used by these cyber-criminals, there could be others which the research intends to unravel.

Attempt to address cyber-crime by various governments and international organizations have not been successful owing to the fact that the identities of the perpetrators of cyber-crime remain ambiguous and inadequate. A study by Zero Tolerance (2006), indicates that cyber-criminals are usually within the age bracket of 18 to 30 years and they indulge in the crime in order to survive and have a taste of good life. Noting these observations, there is need to identify more

attributes/characteristics these cyber-criminals possess and what are other causes since it have been acknowledged that a good taste of life is a major factor.

The internet create unlimited opportunities for commercial, social and educational activities, however, it has introduced its own peculiar risks that pose danger to the economy. This danger could affect many sectors of the society and put the development of the country into peril. Some of these possible adverse effects could include the destruction of the country's image both at home and abroad, insecurity of both life and properties, fear of doing business with Nigerian's citizen, economic loss of spending substantial amount of money on the prevention and control of cyber crime amongst others. For example, a survey on cyber-crime conducted in 2001 by Confederation of British Industry (CBI) and other parties including Price water house Coopers, states that cyber-crime could hinder the growth of e-business because it makes people to be afraid (Broadhurst and Grabosky, 2005). In essence, what other menace does cyber-crime poses to the society.

Consequently, many countries have intensified efforts in curbing the excesses of cyber-criminals. Nevertheless, efforts have been made by the Federal Government of Nigeria to curb the menace of the crime too. For instance, according to Awe (2009), the government of President Olusegun Obasanjo in 2003 set up a working group known as the Nigeria Cyber Crime Working Group (NCWG) to address this phenomenon since the loss suffered by both consumers and investors creates serious credibility and image problem to the country. Similarly, according to Abdulhamid *et al*, (2011), in Nigeria, a bill title "Cyber Security and Critical Infrastructure bill" is presently been prepared to deal specifically with the menace of cyber-crime. The Economic and Other Financial

Crime Commission (EFCC) and the Nigerian Police Force (NPF) have also played vital roles in curbing this menace. To support their efforts, Microsoft and other internet related organizations like PARADIGM Initiative Nigeria, Background Check International (BCI) and the Internet safety, Security and Privacy Initiative for Nigeria (ISSPIN) have also assisted to curb the maladies (Awe, 2009). In spite of all these efforts, cyber-crime in Nigeria is still on the increase. The situation raises a question on the type of cyber-crime that is on the increase and remedy to solve the menace. Consequently, base on the above statements the research work was designed to provide answers to the research questions raised and also to suggest solutions to the problem.

1.3 Research Questions

1. What is the pattern of cyber-crime in tertiary institutions in Zaria?
2. What are the social attributes of those involved in cyber-crime in tertiary institutions in Zaria?
3. What are the factors responsible for cyber-crime in the study area?
4. What are the types of cyber-crime common among cyber-criminals in tertiary institutions in Zaria?
5. What are the consequences of cyber-crime in the study area?
6. How can cyber-crime be curtailed?

1.4 Aim and Objectives of the Study

The objectives of the study are as follows:

1. To find out the pattern of cyber-crime in tertiary institutions in Zaria.

2. To explore the social attributes of those involved in cyber-crime in tertiary institutions in Zaria.
3. To identify the causes of cyber-crime in the study area.
4. To identify the types of cyber-crime that is common in the study area.
5. To examine the consequences of cyber-crime in the study area.
6. To suggest appropriate solutions to the problem.

1.5 Significance of the Study

With the ever increasing pace of development, cyber-crime has become an inevitable and a more specialized area of crime which threatens the economy and even the peace and security of the nation. The publicity surrounding Nigeria cyber-crime is raising fears that the country may face a slowdown in international investment in telecommunication as well as the financial sectors (Thomas, 2011). As more Nigerians use the internet for their banking needs, the number of fraudsters eyeing people's bank accounts and online financial transactions has also multiplied. Hence, this study has provided useful information on the factors responsible for the increase rate of cyber-crime in the society.

Unlike the advance societies, developing societies have almost little or no modalities put in place to curb the excesses of cyber-criminals. In order to out smart the cyber-crime fighting agencies, these cyber-criminals have connections with one another thereby learning more sophisticated methods/skills day in day out to commit this havoc. As such, the exposure of the techniques been

used by these cyber-criminals will contribute positively to the efforts being made by these agencies.

Moreover, since youths within the age bracket of 18-30 years (Zero Tolerance, 2006), have been identified to be most vulnerable to this crime and have also been identified to be either in tertiary institutions or about to be admitted into one or graduates. The research work was able to identify other attributes/characteristics of cyber-criminals. In addition, since cyber-crime is denting the country image among the committee of nations and the present administration has vowed to place Nigeria among the top twenty largest economies in the world by 2020. This research will contribute positively to the efforts being made by concerned government and private agencies to develop strategies to combat the menace.

Above all, taking into account that cyber-crime and the underlying criminology behind cyber criminals are very new and there is a relative shortage of available research and literature on the subject. This therefore, makes this study very important because the study has added to the existing literature by revealing a number of different bases on what typically makes and motivates cyber-criminals and also identify the consequences it has in the society.

1.6 Scope of the Study

The study revolves around issues on the pattern and consequences of cyber-crime. It was conducted in Zaria, Kaduna State and limited to students of 3 selected tertiary institutions namely; Ahmadu Bello University, Federal College of Education and Nuhu Bamalli Polytechnic. In addition, other respondents that participated in the study were operators of cyber café, lecturers from

Computer Science Department of the selected tertiary institution and individuals who indulge in cyber-crime. The study was conducted from August 2011 to May 2013.

1.7 Definition of Key Terms

Computer: Computer is described as an electronic machine that works under the control of store information (programs). It accept data (input), store data in the memory and process the data to produce the required result in a specified format as information (output).

Crime: Crime is an act that violates the basic values and beliefs of society. Those values and beliefs are manifested as laws that the society agrees upon. It could also be referred to an act of committing an offence that is not in line with the laid down laws. Crime is a legal concept and has the sanction of the law (Williams in Dambazau et al 1996).

Cyber: Cyber is a prefix referring to anything related to computer or networking. The word as often used with a growing number of times to describe new things that are being made possible by the spread of computer. Cyber can be combined to make words such as cyber-crime, cyber-space and cyber-café.

Cyber crime: Refers to any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet.

Internet: Internet means international communication network. It is a communication network among computers. It is an interconnection of computers across globe.

CHAPTER TWO

REVIEW OF LITERATURE AND THEORETICAL FRAMEWORK

2.1 Introduction

Literature review refers to the critical examination of state of knowledge including substantive findings as well as theoretical and methodological contribution to a particular topic. In line with this definition, the literature reviewed revolved around the exploration of the intrinsic meaning of variables under study such as; origin of internet and cyber-crime, types of cyber-crime, how cyber-crime is committed, those involved in cyber-crime, causes of cyber-crime and finally the consequences it has on the economy.

2.1.1 Origin of Internet

The origin of internet and its associated information technologies is well documented from its military origins through to education, commercial and later social use (Castells, 1997; in Wall, 2007). The internet, which was originally a limited scientific communication network developed by the United State Government to facilitate cooperation among federal researchers and the university research community is now being used by everyone. Fischer *et al* (2008), stated that the Department of Defense started a network in the 1970s called Advanced Research Projects Agency Network (ARPANET). The aim was to establish a means by which secure and resilient communication and coordination of military activities could be made possible. The ARPANET technology would allow communication to be broken up into 'packets' that could then be sent via a range of different routes to their destinations, where they could be reassembled into their

original form. Castells (2002 in Yar, 2006), stated that the system allowed local area networks (LANs) and wide area networks (WANs) to communicate with one another using a new communications rule called the internet protocol (IP) packet. Another objective of ARPANET was to build a computer communication network capable of sending or receiving data over a variety of paths to ensure that network communication could continue even if part of the network was destroyed, such as in a nuclear attack or by a natural disaster.

From the early 1970, further innovations appeared such as electronic mail applications, which expanded the possibilities for communication. Other networks paralleling ARPANET, were also established such as the UK's JANET (Joint Academic Network) and the US's NSTNET (belonging to the American National Science Foundation) (Yar, 2006). By using common communication protocols, these networks could be connected together forming an inter-net, a network of network. As it grew during its first few years, ARPANET enabled researchers at a few dozen academic institutions to communicate with each other and with government agencies on topics of mutual interest. However, with the highly controversial Vietnam War in full swing, ARPANET's e-mail facility began to handle not only legitimate research discussions but also heated debates about United States involvement in Southeast Asia (Bardin, 2007 in Morley and parker 2007).

The internet is the largest and most well known computer network in the world. It is technically a network of networks, since it consists of thousands of network that can all access each other via the main backbone infrastructure of the internet. Typically, individual users connect to the internet by connecting to computers belonging to an Internet Service Provider (ISP) a company that provides internet access usually for a fee. ISP computers are continually connected to a larger

network called a regional network which in turn is connected to one of the major high speed networks within the country called a backbone network. Backbone networks within a country are connected to each other and to backbone networks in other countries. Together they form one enormous network of networks called the internet.

The internet provides a powerful and versatile environment for business, education, culture, entertainment, health care and public health etc. People that communicate with each other electronically may not have the same platform. Cross-platform means that people do not have to use the same kind of operating system to access files on a remote system. An important factor regarding internet access is bandwidth, which determines how much data a connection can accommodate and the speed at which data can be accessed.

Oyewole and Obeta (2002), highlighted some services that the internet offers which are:

- a. Information:** Through the internet one can have access to vast information on any subject imaginable. The internet can offer immediate and richly detailed information about event in other countries that could not be in any way obtainable.
- b. Electronic Mail (E-mail):** The internet offers a means whereby messages can be sent to other individuals very fast. It is a way of sending message or letter from one computer to another. With electronic mail, one can exchange message with other people you have never met, swap data files, pictures or spreadsheet

with friends or mail commercial information and data around the world. Email works in the same way as the ordinary postal mail except that it is faster.

- c. **Online Shopping:** The internet provides an avenue to exchange goods and services. Business organization use the internet to market their product and services. It is also use for auctioning.
- d. **Entertainment:** The internet is a rich and varied landscape for leisure. It has thousand of games, movies, music etc.

Morley and Parker (2007), also stated that internet can be used for a variety of purposes such as exchanging of e-mail and instant messages, participating in discussion groups, chat sessions and video-conferences, downloading software and music, purchasing goods and services, accessing computers remotely and transferring files between internet users. According to Castells (2002 in Yar 2006), government have seized the internet as a tool for political communication; the State can mobilize it to inform citizens, while citizens can also be drawn into a consultative process whereby they voice their opinions, needs and concerns through mechanisms of online consultation, for example, the internet was used during President Goodluck Jonathan 2011 Presidential campaign. More pragmatically, political parties and political organizations (such as pressure groups) have used the internet for purposes of campaigning and recruitment. The internet has also been seen as a means for stimulating citizen's participation and involvement in civic life at the Local level (Carter, 1997). Wong and Wong (2005 in Broadhurst and Grabosky, 2005), in their essay on Cyberspace Governance and Internet Regulation in China stated that the internet has brought people closer together in a virtual world, transcending geographical distance, time, zones, social gaps and cultural barriers.

Neilsons-Netrating (2002 in Broadhurst and Grabosky, 2005), gave the statistic of internet users in 4 countries as at January, 2002; United State of America has 166 million internet users, United Kingdom - 29 million, Japan - 51 million and Germany - 32 million. According to him, the internet affords new opportunity for individual citizens to communicate efficiently with the police. An example is the Internet Fraud Complaint Center, which operates in USA and receives online information from members of the public relating to questionable online activity. Personnel at the centre evaluate this communication and refer them to the appropriate agency or jurisdiction.

Internet was felt in Nigeria after the evolution of telecommunications especially after 2001 Digital Mobile Licensing (DMC) round by the Nigerian Communications Commission (NCC) opened up the sector. Access to telephone became more profound and soon internet flagged off purely on commercial levels when several ISPs had the political and financial wills to open up for businesses, after due licenses by the NCC. In Nigeria, the number of internet user has grown from a paltry 100,000 in 2004 to more than 7 million in 2010 (Akpore, 2011). He further stated that access to internets has also grown with the reality of blackberry and other modems deployed for Internet connectivity, the numbers of users will be more than double by the end of 2011. With the increasing rate of internet usages, it becomes necessary that there must be an education about the problems and risks associated with the internet.

2.1.2 Origin and Types of Cyber Crime

According to Schell and Martin (2004), the opportunity for creative computer hardware and software invention became available in the 1960s and 1970s through the academic exploration at the all-male Massachusetts Institute of Technology (MIT) and Technology Model Railroad Club (TMRC). The TMRC was formed in 1946 and continues to this day as an actual model railroad club.

The original members used their skills learned at MIT to employ advance control systems and became the first White Hat Hackers. During this period, the world hacker began to represent a technologically focused individual and the term was applied to those who spent time crawling under the railroad tracks at the railroad club facility with the primary objective of connecting switches to relays with cables. Back in the early 1960 to 1970, a 'hack' meant a prank of the kind that the student and the MIT faculty played on their school or on their rivals.

Early hackers at MIT included Alan Kotok, Stewart Nelson, Richard Greenblatt, Tom Knight and Bill Gosper and they all referred to as White Hats (Furnell, 2002 in Yar, 2006). They worked in the lab for 30 hours plus shift and found the primitive computers so fascinating that they forgot about everything else while they were working on them. They taught themselves to pick locks in the MIT computer science building and this lock picking was not a criminal activity because they felt they were simply putting all available equipment to its best use. The early hackers were not criminals but highly talented programmers committed to finding novel solution to difficult problems. If the type of hardware or software that they wanted was not available, these hackers would develop it.

The search for new solution created a hacker community of people who began to share computer code while building an open and freely accessible body of knowledge among peers. It was the sort of intellectual environment that is afforded to academics and is protected by academic freedom and tenure. Hacking itself has undergone considerable and changes over recent years. Perhaps it was true that for the earlier generation of hackers, crackers and viral-coders, technical knowledge and skills were prerequisite, since they had to rely on either formal training in computing and/or concerted experimentation, trial and error in order to stage attacks. However, as hacking

techniques have evolved, an increasing range of automated software tools have appeared which can perform much of the necessary work (Delio, 2001 in Yar, 2006). This was how cyber-crime started.

The term cyber-crime was first coined by William Gibson in 1982 and then popularized in his 1984 novel *Neuromancer* (Wall, 2007). The term cyber-crime broadly describes the crime that take place within that space and the term has come to symbolize insecurity and risk online (Gibson, 1982). Cyber crime encompasses any criminal act dealing with computers and networks (called hacking) and also includes traditional crimes conducted through the internet. For example; telemarketing, Internet fraud, identity theft and credit card account thefts are considered to be cyber-crimes when the illegal activities are committed through the use of a computer and the internet (McQuade, 2009). NCIS, (1999 in Wall, 2007) referred cyber-crime to signify the occurrence of harmful behaviour that is somehow related to the misuse of a networked computer system. The British Police defines cyber-crime as 'the use of any computer network for crime'. From the definition above, it is universally understood that cyber crime is a crime or an unlawful acts committed on the internet with the aid of a computer.

According to Planetindia (2001), the first recorded cyber crime took place as early as in the nineteenth century. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from the further use of the new technology. This was the first recorded cyber crime in the world.

According to Ophardt (2010), cyber-crimes differ from most terrestrial crimes in four ways namely:

1. They are easy to learn how to commit.
2. They require few resources relative to the potential damage caused.
3. They can be committed in a jurisdiction without being physically present.
4. They are often not clearly illegal.

Shehu (2007 in Umar-Ajjola, 2010), observed that it is impossible to have an exhaustive list of the types of cyber crime because as we discuss now, new forms and trends are developing and some of which may take some time to detect. Aghatise (2006), also stated that there are many varieties of crime that are committed on the internet daily, some are directed to the computer while others are directed to the computer users. Kunz and Wilson (2004), stressed that there exist a constantly expanding list that computer crime or internet crime can take. According to them, the following are types of cyber crime:

- a. **Internet Fraud:** Which is commonly referred to as computer fraud can be described as a form of crime that the subjects uses electronic resources to present fraudulent or misrepresented information as a means of deception. According to Kumar (2006), internet fraud is a form of white collar crime whose growth is as rapid as the growth of the internet itself and he identified the following forms of internet fraud:

- (i) **Email fraud:** This is often referred to as the “Nigeria Scam”. Here the victim who fall prey to this crime will send their money and would never receives their expected fortunes. That is merchandise and services that were purchased or contracted by individual online are never delivered.
- (ii) **Spoofing/Phishing:** Spoofing is a technique whereby a fraudster pretends to be someone else email or website. This act is been carried out by coping the web content of a legitimate website to the fraudster newly created fraudulent website. While phishing refers to the scheme whereby the perpetrator used the spoofed website to dupe the victim into divulging sensitive information such as passwords, credit card and bank account numbers.
- (iii) **Investment Fraud:** This is a form of fraudulent claim to solicit investment or loan or that provides for the purchase, use or trade of forged or counterfeit securities.
- (iv) **Identity theft deception and misrepresentation:** This is another form of computer crime that involves the collection of data about individual. Fischer *et al* (2008), said there are various ways that criminal pursuit information which are from rubbish bin, from security weakness in computer system, stealing data base of customer information using social engineering.
- (v) **Cyber Defamation:** It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. In cyber defamation, the criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a

website. (disgruntled employee may do this against boss and ex-boys friend against girl or divorced husband against wife vice versa etc).

b. Unauthorized Access: This type of crime amounts to electronic intrusion or gaining access into another computer without authorization. An example of unauthorized access is hacking. Krone (2005), defined hacking to the breaking into computer system to build information to demonstrate security fault or for other malicious purposes. Arase and Obaedo (2009), identified the following types of crime under unauthorized access:

(i) Hacking: This involves access without right to a computer system or network. The target of the offence is a computer system or network. Access simply means entering the whole or part of the system and the programs of data it contains.

(ii) Interception: Interception is interception, without right and by technical means, of communication to, from and within a computer system of network. The target of the offence is any form of computer communication. Most frequently it concerns data transfer via public or private telecommunications system.

(iii) Time Theft: Time theft refers to the misuse of a computer network system with intent to avoid payment. This offence normally falls within traditional criminal legislation covering offences such as false accounting, dishonestly obtaining services or deliberately avoiding payment.

c. Theft of Intellectual Property: Often referred to piracy, involves the illegal reproduction and distribution of software application, games, movies and audio CD. Ayantokun (2006), states that internet piracy is the process where copies of the software available online are

downloaded and used without the notification of the original owner. Arase and Obaedo (2009), stated that the reproduction, distribution or communication to the public, without right, of a computer program protected by law is an offence and is referred to unauthorized reproduction.

- d. Computer Related Fraud:** According to Arase and Obaedo, computer related fraud offences are usually covered by the common criminal law definitions of fraud and can be prosecuted as such. The offender's objective may be either to obtain financial gain for himself or simply to cause his victim serious loss. Example of computer related crimes are:
- (i) Cash Dispensers:** Relates to fraud and theft arising from cash dispenser systems. Cash dispenser systems commonly known as Automated Teller Machines (ATM) are usually owned by banks and other financial service organizations and use encrypted computer networks. Access to an ATM machine is usually by a card that requires the input of a person identification number (PIN). Fraud occurs by the cloning or duplication of these cards by intercepting the communication link. This gives access to one financial account.
 - (ii) Computer Forgery:** This is done by the creation of forged devices or the fraudulent alternation of software and hardware in order to commit fraud or theft. For example forgery of software of computer system occurs when data is input to replace other data and to represent the original for a fraudulent purpose. For example, the falsification of electronic serial numbers (ESNs) of cellular or mobile telephones.

e. **Malicious Programs:** These programs are intended to cause electronic resources to function abnormally and prevent legitimate users to computer resources.

Examples of malicious programs are:

(i) **Logic Bomb:** This involves the alteration of computer data or computer programs, without right, by the insertion of a logic bomb. Logic bomb is a logic device input by criminals and is triggered when a computer performs a specific task (for example when a payroll account is run). When triggered, the device becomes active and runs a small program which has a detrimental effect on the performance of the computer. The effect is that the computer may stop completely or the screen may go blank or some data are deleted.

(ii) **Trojan Horse:** Trojan horse describes the alteration of computer data or programs, without right, by insertion of a “Trojan Horse”. As its name implies, a Trojan horse is a hidden program in a computer system which is aimed at the alteration or modification of data or programs. It is often used by criminal hackers to leave a “backdoor” in the protection of systems that allows access with a secret code.

(iii) **Virus:** The alteration of computer data or computer programs, without right, by the insertion or distribution of a computer virus. A computer virus is a computer program or part of a computer program that alters data or programs and compromises the integrity of the system. Computer viruses have become very common because the transfer of infected file from one computer to another (often by means of a flash drive/diskette) causes the virus to replicate. There are

hundreds of different types of virus, each with its own characteristics, but all viruses alter either data file or programs within computer.

(v) Worm: Worm involves the alteration of computer data or computer program, without right, by the transfer, insertion or distribution of a computer worm into a computer network. It is a logical device which is designed to travel through computer networks and corrupt or alter computer database. They occur infrequently and are not as common as viruses.

f. Pornography: The term 'pornography' covers all types of material such as explicit literature (electronic or print), photography, films and videotapes with varying degrees of sexual content. The Internet has provided a free market for this crime as so many pornographic sites are now all over the net.

The most prevalent forms of cyber-crime in the world are website cloning (phishing), financial fraud, identity theft, credit card fraud, cyber-theft, cyber-harassment, fraudulent electronic mails, software piracy and virus/worms/ trojans (Olugbodi, 2010). Olugbodi, stated further that the most common form of cyber crime in Nigeria is probably Fraudulent Electronic mails, referred to as 419 in Nigeria. Apparently the number '419' refers to the article of the Nigerian Criminal Code (part of Chapter 38: Obtaining Property by false pretences; Cheating) dealing with fraud. These usually take the form of emails, letters or faxes in which the recipient is persuaded to advance sums of money with the promise of realizing a significantly larger gain. Similarly, Longe and Chiemeké (2008), listed the categories of cyber-crime common in Nigeria internet landscape as follows; hucksters, fraudsters, piracy and hacking. In the same vein Ribadu (2007), stated that the prominent forms of cyber-crime in Nigeria are cloning of websites, falser representations, internet

purchase and other e-commerce kinds of fraud. Ribadu, stated that through the internet, businesses, learning institutions and government departments have been receiving e-mails from senders (criminal) posing as Nigerian/West-African government or business officials offering to share large sums of money. Noting these various types of cyber-crime common in Nigeria, it becomes necessary to identify the type common in the study area.

2.1.3 TECHNIQUES/SKILLS CYBER-CRIMINALS USE TO PERPETRATE CYBER-CRIME

Ahmed (2010), identified some skills/techniques cyber-criminals use to perpetrate their criminal act. These are:

- a. **Dumpster Diving:** They rummage through trash looking for bills or other paper with your personal information on it.
- b. **Skimming:** They steal credit/debit card numbers by using a special storage device when processing your card.
- c. **Phishing:** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- d. **Changing your Address:**They divert your billing statements to another location by completing a change of address form.
- e. **Old Fashioned Stealing:**They steal your wallets and purses, credit card statements etc. They bribe employees who have access to them to give them needed information.
- f. **Pretexting:** They use false pretences to obtain your personal information from financial institutions, telephone companies and other sources.

- g. Social Network Abuse:** Social networks allow us to keep up with friends, family and colleagues but these websites also serve up our identities on a silver platter to identity thieves. Key personal details such as age, hometown, employer and personal favorites can be used against you. For example, after looking at your profile page for basic information about you, a pretexter could call pretending to be from an organization you trust and ask for important personal data such as your birthday or social security number.

Other techniques cyber-criminals use to commit cyber-crime according to Pati (2005), are:

- h. Email bombing:** This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.
- i. Data diddling:** This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed.
- j. Web jacking:** This term is derived from the term hi jacking. In these kind of techniques, the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money.
- k. Denial of Service attack:** The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. For example, Amazon and Yahoo.

- I. **Theft of information contained in electronic form:** This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

While the tools attackers use to break into networks are as below (Ahmed, 2010):

- a. **Exploit:** An exploit is a piece of software, a chunk of data or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behaviour to occur on computer software, hardware or something electronic. This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.
- b. **Port Scanner:** A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to compromise it.
- c. **Vulnerability Scanner:** A vulnerability scanner is a computer program designed to search for and map systems for weaknesses in an application, computer or network.
- d. **Password Cracker:** A password cracker is a software that recovers secret passwords from data that has been stored in or transmitted by a computer system.
- e. **Network Sniffer:** A program or device that monitors data travelling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network.

Based on the observation raised by Shehu (2007 in Umar-Ajjola, 2010) that it is impossible to have an exhaustive list on the types of cyber-crime so are the

skills/techniques that are used by these cyber-criminals. To fight cyber-crime, those involved must note that it is not one-off but a lifelong because the techniques do changes. Security agents cannot fight today's crime with yesterday technology. It will be a losing battle if security agents are way behind the cyber-criminals in terms of knowledge.

2.1.4 CATEGORIES OF INDIVIDUALS INVOLVED IN CYBER-CRIME

Cyber criminals constitute of various groups/category (Pati, 2005). This division may be justified on the basis of the object that they have in their mind. However, the following are the category of cyber criminals according to Pati:

- (a) **Adolescent:** The simple reason for this type of delinquent behaviour pattern in adolescent is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other youths in their group. Furthermore, the reasons may be psychological. For example Mulhall (1997, in Schell and Martin 2004), stated that we have witnessed an alarming number of young people who for a variety of sociological and psychological reasons have become attached to their computers and are exploiting their potential in a criminal manner such as telecommunications fraud (free long distance phone calls), unauthorized access to other computers (whether for profit, fascination or ego), credit card fraud (cash advances and unauthorized purchases of goods) and the move to other destructive activities like computer viruses.

- (b) **Organised Hackers:** These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. They constitute individual of different ages.
- (c) **Professional Hackers / Crackers:** Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Furthermore, they are ven employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.
- (d) **Discontented Employees:** This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge, they tend to hack the system of their employee.

Report of EFCC (2012), also revealed the categories and ages of individuals involved in cyber-crime; a 25-year-old student of the University of Ilorin name Imonina Kingsley was sentenced to 20 years jail term by Justice Mohammed Shuaibu of Federal High Court in Kaduna. He was charged for the following; impersonation, possession of fraudulent documents and attempt to obtain money by false pretences. Another student name Olasaidi Dare of Olabisi Onabanjo University in April 2012 was caught for offences related to computer fraud and was sentenced to 5 years imprisonment. Also, Abayomi Lawal Adekunle Nurudeen, a final-year student of Survey and Geo-Informatics Engineering at the University of Lagos, was sentenced 19 years in jail for obtaining \$47,900 from Pee Loo Rosalind Summer, an Australian lady. Similarly, Ferdinand Iheasirim, a 1993 graduate of Accountancy of Abia State University had claimed to Rev Robert McArdle, an

Australian and that he was Ben Agwu, a security adviser to Nigeria's president. He was sentenced to 10 years imprisonment.

Olaide and Adewole (2004), observed that a sizeable number of cyber-criminals in Nigeria falls within the youthful age. They further stated that the youths at present have discovered different ways of using the internet in doing different types of criminal activities. Sesan (2010), pointed out that many young Nigerians, like youths everywhere, are unfortunately on the wrong side of the economic divide. He stated that many of them either lack any serious engagement or are greedy to imitate the flashy people they see on television which they have now adopted as mentors and these age bracket who are the main perpetrators are usually found in tertiary institutions in Nigeria. Ribadu (2007), stated that in most Nigeria tertiary institutions various form of crimes are being witnessed daily ranging from examination malpractices, falsification of admission, rape, robbery and stealing, sexual abuse, assault, cultism amongst others. But in recent times cyber-crime now exists in out tertiary institutions. Students of tertiary institution now engage in cloning of websites, falser representations, internet purchase and other e-commerce kinds of fraud such as credit card fraud. Aside the above listed actors involved in cyber-crime, are there other actors and what other social attributes do these criminals possess?

2.1.5 CAUSES OF CYBER CRIME IN NIGERIA

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in the cyberspace, (Hidayatullah, 2000). However, scholars have attributed the causes

of cyber-crime in Nigeria to the following: Okoro (2010), identified the following as the causes of cyber-crime in Nigeria: unemployment, negative role models, lack of adequate policing facilities and knowledge of cyber crime and social gratification. According to him, all these reasons serve to facilitate cyber crime in Nigeria. Also, Awe (2009) stated that the widespread of corruption, harsh economic climate, high unemployment, disregard for the rule of law and lack of transparency and accountability in governance are the main cause of cyber-crime in Nigeria.

Babt (2008) added that cyber-crime in Nigeria can be associated with two causes which are the primary and secondary causes. The primary causes include high unemployment rate, harsh economic condition, prevalence of poverty and weak educational system. The secondary causes can be traced to greed, corruption and get rich quick syndrome. Ayantokun (2006), highlighted high level of corruption and wide spread of poverty as the main cause of cyber-crime among Nigerian youths. Many Nigerians are said to be living below the poverty line (below one dollar per day) (Ogbunwezeh, 2006). Akande (2007) further stated that over 5 million Nigerians youths are job seekers and that thousands and thousands of graduates of tertiary institutions are released each year to the job market. When it is difficult to get job, they result to other means.

2.1.6 CONSEQUENCES OF CYBER-CRIME ON NIGERIA ECONOMY

Life is about a mix of good and evil. So is the Internet. Despite its advantages the internet has its dark sides too. Cyber-crime is not without costs and these costs increase daily. These losses manifest themselves in various ways such as loss of life, loss of dignity and loss of employment. The impact cyber-crime has, however, is not only limited to the victims, it spreads its impact to the

society as a whole. Ringwelski (2008) explained the consequences cyber-crime has on the economy. These are:

- a. **Loss of Revenue:** One of the main effects of cyber-crime on an economy is the loss of revenue. For example, in financial institution or multinational companies' loss of revenue can be caused by an outside party who obtains sensitive financial information and using it to withdraw funds. It can also occur when a business's e-commerce site becomes compromised while inoperable, valuable income is lost when consumers are unable to use the site. It is also applicable to the individual.
- b. **Wasted Time:** Another major effect or consequence of cyber-crime is the time that is wasted when IT personnel must devote great portions of their day handling such incidences. Rather than working on productive measures for an organization, many IT staff members spend a large percentage of their time handling security breaches and other problems associated with cyber-crime. Waste of time could also be viewed when international banks often delay Nigerian financial transactions, pending proper verification.
- c. **Damaged Reputations:** In cases where customer records are compromised by a security breach associated with cyber-crime, a company's reputation can take a major hit. Customers whose credit cards or other financial data become intercepted by hackers or other infiltrators lose confidence in an organization and often begin taking their business elsewhere. Due to these, foreign investors often consider Nigeria as an unattractive market and it has detrimental impact on Nigerian citizenry when they travel outside to do business.
- d. **Reduced Productivity:** Due to the measures that many companies must implement to counteract cyber-crime, there is often a negative effect on employees' productivity. This is because, due to security measures, employees must enter more passwords and perform

other time-consuming acts in order to do their jobs. Every second wasted performing this task is a second not spent working in a productive manner.

The impacts of cyber-crime already have detrimental influence on Nigerian citizenry/economy. Global anti corruption bodies, such as Transparency International and the FATF, have listed Nigeria as one of the most corrupt countries in the world (Oyesanya, 2004). Private companies around the world are beginning to take steps geared at blocking email traffic originating from Nigeria. Nigerian financial instruments are now accepted with extreme due diligence around the world and some international banks have completely denied access to their web sites if the traffic originates from Nigeria. Cyber-crime might also hinder technological development within Nigeria (Awe, 2009).

In conclusion, studies conducted on cyber-crime in Nigeria concentrated on some geographical areas forgetting that it is a global issue which needs to be tackled. Noting this gap, it becomes imperative to identify the types of cyber-crime committed in the study area, the techniques used and other actors involved in cyber-crime including the social attributes they possess. Nonetheless, the study is interested in looking at the problems faced by the youth that predisposed them in engaging in the crime.

2.2 Theoretical Framework

McQuade (2006), defined a theory as an interrelated and testable set of propositions that explain a phenomenon. Osuala (1992), also defined a theory to be an attempt at synthesizing and

integrating empirical data for maximum clarification. In the same view, Haralambos and Holborn (2008), also defined sociological theories to be a set of ideas that provide an explanation for something. In order to understand and explain the initial involvement of student and continuation of cyber-criminal in the society, differential association theory was adopted.

DIFFERENTIAL ASSOCIATION THEORY

The theory was developed by Edwin Sutherland in 1939. He coined the phrase “differential association” to address the issue on how people learn deviance. This theory explains deviance in terms of the individual’s social relationships. According to this theory, the environment plays a major role in deciding which norms people learn to violate. Specifically, people within a particular reference group provide norms of conformity and deviance and thus heavily influence the way other people look at the world, including how they react. People also learn their norms from various socializing agents such as the parents, teachers, friends, co-workers and the media. In short, people learn criminal behavior, like other behaviors, from their interactions with others, especially in intimate groups.

The principle of differential association asserts that a person becomes delinquent because of an “excess” of definitions favorable to violation of law over definitions unfavorable to violation of law. What this means is that an individual will become a criminal because they are exposed to more favorable criminal influences rather than more favorable legal influences. In other word, criminal behavior emerges when one is exposed to more social message favoring conduct than pro-social messages. This can be seen in environments with poor socio-economic conditions which may encourage negative views towards the law and authority.

This theory is significant because it puts an individual's social environment into context as a means to explain why some individuals engage in criminal behavior. The theory has the following assumptions:

1. Criminal behavior is learned. This means that criminal behavior is not inherited, as such; the person who is not already trained in crime does not invent criminal behavior. This assumption proposes that individuals are inherently good and only turn towards deviant behavior as a result of learning the behavior.
2. Criminal behavior is learned in interaction with other persons in a process of communication. According to Sutherland, this would mean that an individual is influenced to participate in criminal behavior through watching and interacting with other individuals who are engaging in the criminal behavior.
3. The principal part of the learning of criminal behavior occurs within intimate personal groups. This would be any group that has a significant influence over them, such as their family or close friends. This factor makes a great deal of sense since the process of socialization and growing up is heavily influenced by the groups of people that an individual is a part of. Most families try to institute a positive influence on a member of their own, however, if a juvenile comes from a family that is broken and develops strong emotional ties with friends engaged in deviant behavior then this is likely to also drive them into the same deviant behavior, according to Sutherland.
4. When criminal behavior is learned, the learning includes techniques of committing the crime, which are sometimes very complicated, sometimes simple and they learn the specific

direction of motives, drives, rationalizations and attitudes for committing a crime. This means that an individual will be influenced into believing that the behavior which they may have previously believed was wrong, into believing that it is right through rationalization of their action. For example an individual from a disadvantaged background may rationalize cyber-crime as taking from those who have wealth in order to make things fair.

5. The fifth factor states that an individual will be pushed into deviant behavior depending on their view of the legal code as being favorable or unfavorable. This states that an individual may be driven into deviant behavior, if they see the laws as being tough and unfair. This would influence their rationalization for breaking the law since they view it as unfair.
6. A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of the law. This is a core component of Differential Association and it states that an individual will break a law if they see more reasons to break it than to stay in compliance with it. In their minds, an individual would take a look at a law and compare the rewards for both actions and make their decision based on the one which would benefit them the most. They may see cybercrime as having a financial benefit for them, but they would also see a prison term as a potential ramification and make their decision accordingly. It is when an individual views breaking a law as having a greater benefit for them than keeping it that results in deviant behavior.
7. Differential associations may vary in frequency, duration, priority and intensity. This factor would be attributed to how strong their bond is with the individuals they interact with who commit the criminal behavior. If they interact on a daily basis and have strong emotional ties then they are likely to commit the deviant behavior more frequently than they otherwise would have.

8. The process of learning criminal behavior by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning. This means that individuals learn criminal actions and legal actions through the same way. An individual would learn behavior that is counter productive to society in the same way that they would learn behavior that is productive. This is why an individual would learn criminal behavior through their interactions with others.

9. The final postulation of differential association theory states that while criminal behavior is an expression of general needs and values, it is not necessarily the fulfillment of these needs and values which causes deviant behavior since non-criminal behavior is an expression of these same needs and values. An example of this is the need for an individual to be accepted and loved. Sutherland argues in this factor that it would not necessarily be the fulfillment of being accepted and loved which leads an individual to deviant behavior since non-criminal behavior also can fulfill the requirement to be accepted and loved.

This theory, which was developed to help explain white collar crime, fits in well with those who violate or commit cyber-crime. According to a research conducted by Imhof (2010), he states that a lot of hacking of systems occur during college. Some of these individuals spend time with people who share similar interests. It is in these groups where the third factor of differential association can be applied which deals with learning deviant behavior as part of a close group. These groups may serve a well meaning purpose such as research or otherwise hacking of systems. However, being part of this group may lead a well intentioned individual to commit a crime if they are influenced by other members of their group which are doing so. It is through these groups, that an individual would learn the techniques which would help them perfect their craft. It would also be

through these means that they would develop a rationalization for illegal compromising systems. In addition, according to the seventh postulation of differential association, the more time an individual would spend with members of these groups who are committing illegal acts; it would also increase the frequency that they engage in deviant behavior.

However, one of the major criticism of the theory is that the theory focuses on how individuals learn how to become criminals but does not concern itself with why they become criminals. This means that there are other push factors such as economic, sociopolitical and cognitive that push an individual to commit cyber-crime. For example, an individual may be a good person who through, perhaps no choice of theirs, is put into a poor socio-economic climate with an atmosphere of deviance. Such individual will be willing to learn the crime by associating himself with cyber-criminals. Here the cyber-criminal becomes self motivated and a rational actor.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter focuses on the valid approach used in obtaining accurate data to produce precise results in providing answers to the research problem (Akpabio and Ebong, 2009). It also provides a comprehensive and detailed description on how the required data were collected and analyzed. Stanley in Erinosho *et al* (2002), stated that methodology is important because it enables us to ask and also to begin to answer (these) interesting and important questions such as; who are cyber criminals, what techniques do they use to get their victim, what age bracket are involved in cyber-crime amongst other. Therefore, this chapter will provide a detail step by step description of every procedure used in carrying out the research study. The chapter entails description of the location of study, types and sources of data, techniques of data collection, population and sampling and techniques of data analysis.

3.2 Location of the Study

Zaria is a city in Northern Nigeria and it is located in Kaduna State. Zaria which used to be known as Zazzau at an earlier time is located within latitude $11^{\circ} 3'N$ and $11^{\circ} 15'N$ and longitude $7^{\circ} 42'E$

and $8^{\circ} 45'E$ of the Greenwich Meridian. Zaria is 80km north of Kaduna along the federal high way leading to Kano. The settlements extend to the north by Giwa along Funtua-Katsina road, to the south by Kachia, to the east by Kabau along Saminaka and to the west by Birnin Gwari. It was founded as one of the seven states of Hausa (Hausa Bakwai). The city was annexed into the Songhai Empire in the 16th Century. Afterwards, the Fulani conquered it in the early 19th Century. The British gained control over Zaria in 1901. The majority of the inhabitants are Muslims. The current Emir of Zazzau (*Sarkin Zazau* in Hausa language) is HRH Alhaji Shehu Idris. Zaria has 2 local government areas namely Zaria city LGA and Sabo-garin LGA.

Zaria is the second largest city in Kaduna State and in 1991 census with a total population of about 489,858 people. In 2006 census, the population was about 501,198 people. Based on an estimated growth rate of 2.3% the present population of Zaria is about 558,836 people (Census 1991 and 2006). The economy of Zaria is based primarily on agricultural and industrial development. The major agricultural products in Zaria are cotton, peanuts, hides and skins, ginger, beeswax and durra sorghum. The industries in Zaria comprise of cotton ginning, peanut and shea-nut milling, tanning, cottonseed-oil milling and the manufacture of cigarettes, perfumes and soap. In addition, economic activities are small scale business, blacksmithing, trading and knitting.

The largest river in Zaria is the Galma River and it is located close to Zaria city. It originates from Jos, Plateau state and it carries water throughout the year (Mortimore, 1970). Also, the vegetation of Zaria is of the guinea savanna characterized with more of shrubs and grasses. There are also educational institutions in Zaria namely; Ahmadu Bello University, Nigerian College of Aviation Technology, National Research Institute for Chemical Technology, Federal College of Education,

Nuhu Bamalli Polytechnic, National Institute of Transport Technology amongst others. Zaria was chosen for the study because of the large presence of tertiary institutions and these tertiary institutions consist of students who represent the largest users of the internet and have also been identified to be the major perpetrator of cyber-crime.

The study was conducted in 3 tertiary institutions in Zaria. These institutions are; Ahmadu Bello University Zaria, Federal College of Education Zaria and Nuhu Bamalli Polytechnic. These 3 tertiary institutions were selected because they represent the types of tertiary education that most of the individuals attend to acquire knowledge and also because of the large presence of students.

3.2.1 Ahmadu Bello University, Zaria

The Ahmadu Bello University, Zaria (ABU) was founded on October 4, 1962 as the University of Northern Nigeria by the then Northern Region government. ABU began full operation on the sites of these educational institutions: the defunct Nigerian College of Arts, Science and Technology, founded in 1955; the Clerical Training Centre, Kongo, founded in 1957; the Samaru Agricultural Research Station, established in 1924 and the Shika Livestock Farm, started in 1928. ABU began with the faculties of Agriculture, Engineering, Law and Sciences, 15 academic departments and 426 students. ABU was later taken over as a Federal Institution in 1975 through a Decree (Ahmadu Bello University Transitional Provisions Decree of 1975), thus becoming a Federal University. As stated in Part (ii) of its Principal law, the University was created to, among other things, produce

high level manpower, secure the diffusion of knowledge, research and community service in Northern Nigeria and Nigeria in general and to function as a center of excellence.

From a modest beginning in 1962, by 2002 the University has been transformed into the largest and the most extensive of all Universities in Sub-Saharan Africa. Currently, the University covers a land area of 7,000 hectares and encompasses 2 campuses, 12 academic faculties and a Postgraduate School. It also has 5 Institutes, 6 specialized centers, a Division of Agricultural Colleges, a Demonstration Secondary School, a Primary School and Extension and Consultancy Services, which provide a variety of services to the University and the wider society. There are about 1,400 academic and research staff and 5,000 support staff serving the University. The University has also nurtured 2 University Colleges namely; Abdullahi Bayero College (now Bayero University, Kano) and Abubakar Tafawa Balewa College (now Abubakar Tafawa Balewa University of Technology, Bauchi). While 27 tertiary Institutions made up of Colleges of Education, Polytechnics and Schools of Basic of Preliminary Studies are affiliated to it. The university has about 30,081 students (MIS, 2012).

3.2.2 Federal College of Education Zaria

The Federal College of Education Zaria (FCE) was formerly known as the Advanced Teachers' College. The college was formally opened on 1st November 1962 with an initial intake of 150 students. The College was established along side with 3 other Advanced Teachers' Colleges located in Lagos, Owerri and Ondo in order to meet the rapid expansion of secondary school. The College name was later changed to Zaria Teachers' College and in 1991 was renamed Federal College of Education, Zaria. At take off, the College was established to fulfill the following objectives; to provide professionally qualified non-graduate teachers of Northern Region origin to

man the secondary and teacher training colleges in the region, to provide professionally qualified assistant inspectors for primary schools and finally through the products of the college, to be able to gradually northernise the entire staff of all the secondary schools and teacher training colleges in the region.

With the creation of more states in the Federation, the College became the property of the former six Northern States. The duty of administering the College in the interest of the six Northern States fell on the Interim Common Services Agency (ICSA) which in 1970 specifically requested the Institute of Education ABU to take over the administrative control of the College. The College was temporarily situated in the present site of Kaduna State polytechnic along Gaskiya Road, Zaria opposite the Institute of Education, ABU Annex. But due to the expansion of the College, in January 1973, the College moved to its present site along old Jos road.

Academically, the College is organized into Schools and each headed by a Dean. The School is made up of a number of departments of related subjects. The affairs of the department are managed by Head of Department and co-coordinating lecturers. The Provost is both the Administrative and Academic Head of the College. He is assisted by the Deputy Provost who deputizes in his absence. The College has 6 Schools namely; School of Arts and Social Sciences, School of Education, School of languages, School of Sciences, School of Vocation and School of undergraduate Studies. The College also has about 8,645 students (MIS, 2012).

3.2.3 Nuhu Bamalli Polytechnic

Nuhu Bamalli Polytechnic (NBP) came into being on the 2nd of February, 1989 vide Kaduna State Edict No. 3 (subsequently amended in 2004). The Edict charged the Polytechnic to among other things provide for training and development of techniques in Applied Science, Engineering and Commerce as well as in other spheres of learning. The Polytechnic courses of instruction (in full-time and Part-time) leading to the award of Diplomas, Certificates and other distinctions of Scientific, Technological and other subjects are available at all times in order to meet the requirements of State and the manpower needs of the Country.

The School is been administered by a rector. NBP has the main campus located along Zaria-Kaduna express way, the annex campuses located along Gaskiya Road, Zaria opposite the Institute of Education, ABU Annex, and Samarun Kataf campus. NBP also has the following School: School of Management Studies, School of Applied Sciences, School of Liberal Studies, School of Engineering Technology, School of Environmental Studies and School of Agricultural Technology which is located in Samarun Kataf campus. The polytechnique has about 10994 students (MIS, 2012)

3.3 Types and Sources of Data

Data for this study were collected from primary source. The primary data that were used for this study were collected through survey and in-depth interview. The primary data were drawn from students, lecturers from Computer Science Department in the 3 selected tertiary institutions,

operators of cyber-café within Zaria and cyber-criminals. The questionnaires were administered to students of selected tertiary institutions in the study area while the in-depth interview was conducted with lecturers, operators of cyber-café and cyber-criminals.

3.4 Techniques of Data Collection

In order to collect reliable data and capture the range of information required in pursuance of the research objectives, both quantitative and qualitative techniques of data collection was used. The quantitative data was obtained through survey by administering questionnaires. Ogunleye (2000 in Olayiwola, 2007), defined questionnaire as an instrument used for getting answers to a set of questions by using a format which the respondents fills by themselves. Through the questionnaire, detailed and reliable information was obtained from students of tertiary institutions. The questionnaire was structured in such a way that it contained both open and closed ended questions. The reason for the open ended questions was to allow respondents express their views on the subject matter while closed ended was to enable the respondents select among the various option the researcher provided. The questionnaire was divided into seven (7) sections which are as follows; section A deals with the socio-demographic characteristics of the respondents, section B was on the pattern of cyber-crime, section C was on the types of cyber-crime common in the study area, section D deals with the social attributes of cyber-criminals while section E contained the causes of cyber-crime. Section F and G was on the consequences of cyber-crime and solution to the problem respectively.

The qualitative data was obtained through In-depth interview. The qualitative technique concentrates on collecting quality information mainly from a relatively much fewer individuals

(Gyong, 2011). Chantler (1996 in Rogers 2001), believed that qualitative-based research is an appropriate approach when attempting to discover intricate details of phenomena that are difficult to convey with quantitative techniques. The qualitative technique was used to complement the quantitative technique. Akpabio and Ebong (2009), define in-depth interview as the process where the researcher collects data by means of verbally asking relevant questions to meet the research objectives. The in-depth interview was structured and designed to elicit information from lecturers of Computer Science Department, operators of cyber-café and cyber-criminals. Operators of cyber-café were chosen because of the client-server relationship between cyber-criminals and operators of cyber-café while lecturers of Computer Science Department were chosen because of their knowledge on the subject matter. Finally, cyber-criminals were selected due to the fact that they will be able to give intrinsic details of the crime. The in-depth interview focuses on the pattern of cyber-crime, motivating factors, types been perpetrated, social attributes of cyber-criminals and solution to the menace.

3.5 Population and Sampling Procedures

Sampling refers to the process of selecting a sample or a subset or a portion of the population to represent the entire population in a study (Akpabio and Ebong, 2009). Considering the nature of the study, the population for the study was divided into 4 categories. The population for the first category was drawn from students within the selected tertiary institutions; the population for the second category was drawn from operators of cyber-café while the population of the third category was drawn from the lecturers of computer science department of the selected tertiary institutions. The population for the last category was drawn from cyber-criminals within the study area.

For the purpose of this study both probability and non-probability sampling techniques were used to select the respondents. The probability sampling method that was used is the simple random sampling while the non probability sampling methods was the purposive and snowball sampling. Students from the 3 selected tertiary institutions were selected using simple random sampling. Operators of cyber-café and lecturers from computer science department were selected using the purposive sampling method while cyber-criminals were selected using the snowball sampling method.

There are various tertiary institutions within Zaria namely: Ahmadu Bello Univerisity, Nigerian College of Aviation Technology, National Research Institute for Chemical Technology, Federal College of Education, Nuhu Bamalli Polytechnic, National Institute of Transport Technology, Institute of Agricultural Research. Three (3) tertiary institutions namely: Ahmadu Bello Univerisity, Federal College of Education and Nuhu Bamalli Polytechnic were purposively selected because of the large population of students and the relevance of this tertiary institutions to the investigation under study.

In order to get the sample size of the first category of respondents, the student's population was obtained from the Management Information Services (MIS) of each of these selected institutions. The population of the students was based on 2011 – 2012 academic session. Thereafter, the Yamane's formula was used to get the sample size.

$$n = \frac{N}{1 + N(e)^2}$$

Where: n = sample size

N = total population

e = level of significance (0.05)²

ABU has a total population of about 30081 students

FCE has a total population of about 8645 students

Nuhu Bamalli Poly has a total population of about 10994 students

$$n = \frac{49720}{1 + 49720(0.05)^2}$$

Approximate 396.80 to the nearest hundred = 400

The questionnaires were then administered to the 3 selected tertiary institutions in the following order based on their population:

ABU

$$\frac{30081 \times 400}{49720} = 242 \text{ questionnaires}$$

FCE

$$\frac{8645 \times 400}{49720} = 69.5 \text{ to the nearest whole number } 70 \text{ questionnaires}$$

Nuhu Bamalli Poly

$$\frac{10994 \times 400}{49720} = 88 \text{ questionnaires}$$

From the above calculation, ABU with a population of about 30081 students accounts for 242 questionnaires (60.5%), FCE with about 8645 students accounts for 70 questionnaires (17.5%) and Nuhu Bamalli Poly with about 10994 students account for 88 questionnaires (22%). The distribution of questionnaires to respondents is as follows:

- (a) **ABU Zaria:** ABU Zaria consists of 12 faculties namely; Faculty of Administration, Agriculture, Arts, Education, Engineering, Environmental Design, Medicine, Law, Pharmaceutical Sciences, Science, Social Sciences and Veterinary Medicine. Out of the 12 faculties in ABU Zaria, 2 faculties were selected for the study using simple random sampling. The selection was done by giving each faculty a serial number 1 to 12 and thereafter, 2 faculties were picked through simple balloting without replacement. This was done by writing 'Yes' on 2 slips of paper and 'No' on 10 slips of paper making a total of 12 slips of paper, folded and then shuffling them into a container. The slips are then drawn and whichever faculty picks yes was selected for the study. By so doing, it gives all faculties an equal opportunity of being selected for the study without avoidance of bias. After the shuffling and selection, the following faculties were selected: Faculty of Education and Faculty of Science. The questionnaires were administered equally between the 2 faculties. Faculty of science has nine (9) departments namely Biochemistry, Biological Science, Chemistry, Geology, Geography, Mathematics, Microbiology, Physics and Textile Science and Technology. Five departments were selected using simple

balloting without replacement and the departments selected are: Biochemistry, Geology, Geography, Mathematics and Physics. Twenty (24) questionnaires were administered to four departments while 25 questionnaires were administered to Mathematics department. Faculty of Education has the following Departments; Science Education, Guidance and Counseling, vocational and Technical Education, Physical Health Education, Curriculum and Instructional Education and Psychology Education. 20 questionnaires were administered equally among the departments with exception to Science Department that 21 questionnaires were administered.

(b) FCE Zaria: The College consists of the 6 Schools namely; School of Arts and Social sciences, Education, Languages, Sciences, Vocations and undergraduate Studies. All the Schools were given a serial number from 1 to 6 and thereafter, 2 Schools were picked using the same process indicated above. The Schools selected after a reshuffle are School of Languages and School of Sciences. The questionnaires were divided equally among the Schools selected. For the School of Science, the questionnaires were administered equally among the departments which are Biology, Chemistry, Computer, Integrated Science, Mathematics, Physical Health Education and Physics Department. While 6 questionnaires were administered each to Arabic, English, French, Hausa and Igbo Department with exception to Yoruba Department that got 5 questionnaires.

(c) Nuhu Bamalli Polytechnic: Nuhu Bamalli Polytechnic consists of 6 Schools namely; School of Management Studies, Applied Sciences, Liberal Studies, Engineering Technology, Environmental Studies and Agricultural Technology. All Schools were given a serial number from 1 to 6 and thereafter, 2 Schools were picked using the same method indicated above. The selected Schools are School of Management Studies and School of Liberal Studies. The

questionnaires were divided equally among the Schools selected. Thereafter, 11 questionnaires were administered each to Accounting, Banking and Finance, Business Administration and Public Administration for School of Management Studies. School of Library Studies is on its own.

In-depth interview: 4 respondents were purposively selected from the second category of respondents which are the operators of cyber-café within Zaria. The selection of respondents for the in-depth interview was purposive because only cyber-cafes that were identified to have adequate computer facilities, popular and frequently patronized were selected. In addition, 6 respondents that is 2 respondents each from the selected tertiary institutions were purposively drawn from the third category. There selection was also purposive based on the respondent's knowledge on the subject matter. Finally, 2 respondents were selected from the fourth category of the population using the snowball sampling method. The first cyber-criminal that participated in the research was identified with the assistance of an operator of cyber-café. Thereafter, the second cyber-criminal was identified with the assistance of the first cyber-criminal.

3.6 Techniques of Data Analysis

The study involves the use of quantitative and qualitative instruments as such both quantitative and qualitative techniques of data analysis were used. Data collected through quantitative instrument (questionnaires) was subjected to simple statistical analysis and interpretation. A code book was manually prepared to organize the data collected and the information was transferred to a code sheet. It was then analyzed with the aid of a computer using the Statistical Package for Social Sciences (SPSS version 17.0). The SPSS was used to generate frequencies and percentages.

While data collected through the qualitative instrument (in-depth interview) was transcribed from field notes and tapes. All categories of responses were merged and compared in order to bring out emerging themes. The entire process was guided by the objectives of the study.

3.7 PROBLEM ENCOUNTERED IN THE FIELD

The problem that was encountered in the field was the refusal of cyber-criminals identified to participate in the study due to fear of being arrested. While the 2 cyber-criminals that participated in the research requested for money before they granted audience.

CHAPTER FOUR

FINDINGS ON CYBER CRIME IN TERTIARY INSTITUTIONS IN ZARIA

4.1 INTRODUCTION

The contents of this chapter are the analyses and interpretation of the quantitative and qualitative data collected from the field. This was done thematically using the objectives of the study in order to present the data adequately. This chapter comprises of seven sections which are; the socio-demographic characteristics of the respondents, the pattern of cyber-crime, the types of cyber-crime common in Zaria, the attributes of individuals involved in cyber-crime, factors

responsible for individual involvement in cyber-crime, implications on the society and finally, solutions to the menace.

The study adopted the use of triangular method in the analyses and interpretation of data. The triangular method involves the combination of both quantitative and qualitative method in the interpretation of the findings collected from the field. This method automatically increases the validity of the study as findings from the various methods of data collection complement each other. Analysis and interpretation was based on 400 questionnaires administered and 12 key informants that were interviewed.

4.2 SOCIO-DEMOGRAPHIC CHARACTERISTICS OF RESPONDENTS

This section presents the socio-demographic characteristics of the respondents. The socio demographic characteristics of respondents analyzed are sex, age, religion and marital status and they were presented in prose form.

Socio-demographic Attributes of Respondents. Findings from the quantitative data showed that 75% of the respondents are males while 25% are females. The age distribution of respondents was also obtained. From the data, the respondents within the ages of 18 – 24years were of the highest number representing 58%. This is followed by respondents who are of the ages of 25 – 30years representing 32%. While the ages 31 – 35years and 36years and above were 5% each representing the lowest age of respondents. This indicates that most of the respondents who took part in this study were young adults.

The data obtained also disclosed the religion background of the respondents. It was found that 56% of the respondents are Muslims while 41% are Christians. Only 3% are practicing traditional religion. Finally, on the marital status of the respondents, 82% of the respondents were single while 17% are married. Only 1% of the respondents were divorced and none were widow.

4.3 PATTERN OF CYBER-CRIME IN TERTIARY INSTITUTIONS IN ZARIA

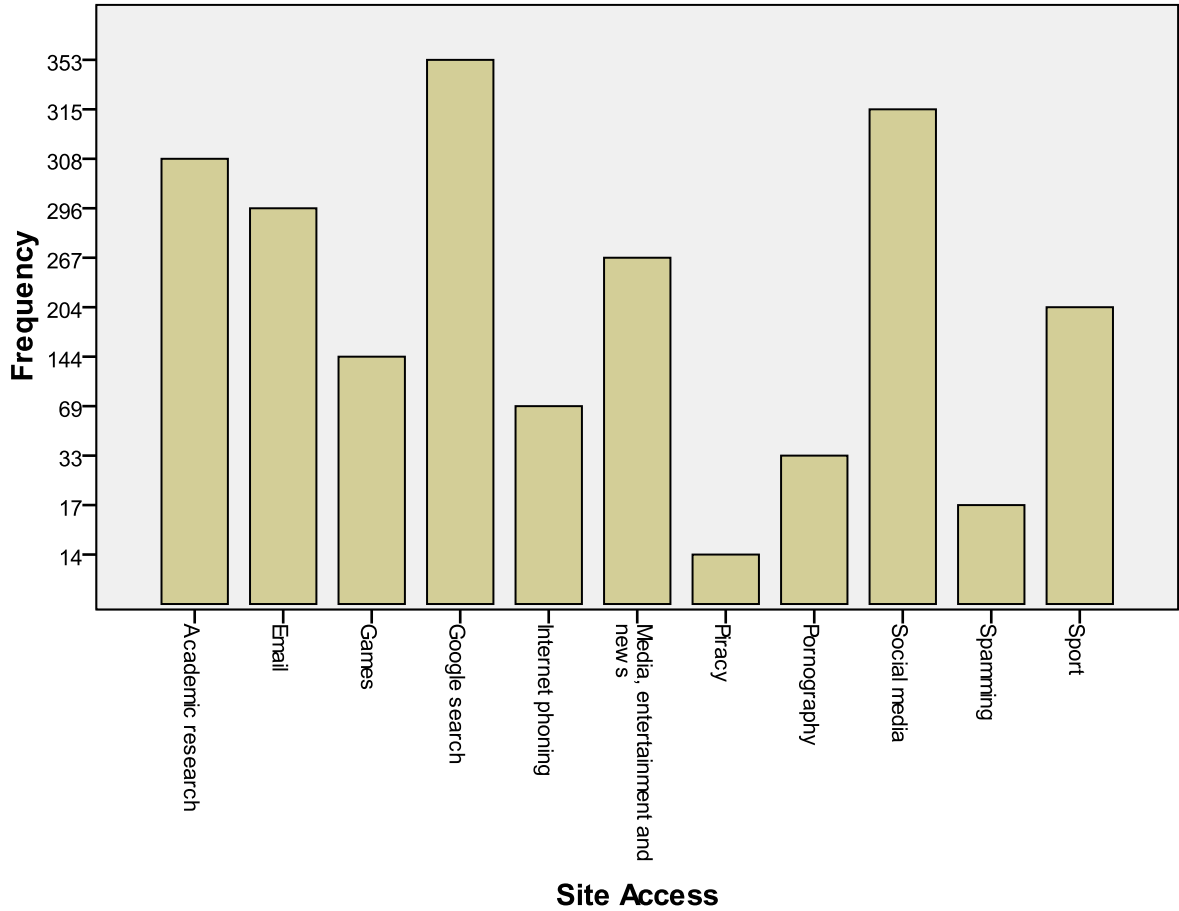
This section found out the pattern of cyber-crime in tertiary institutions in Zaria. Pattern identified are; individuals involved in the crime, time of perpetration, perpetration point, frequency of occurrence and techniques used to perpetrate the act.

Table 4.3.1: Access to Internet

Access to internet	Frequency	Percentage
Yes	396	99.0
No	4	1.0
Total	400	100.0

Table 4.3.1 shows the respondents views if they access the internet. The finding reveals that majority of the respondents access the internet. This implies that the respondents use the internet for one activity or the other.

Figure 1: Respondents' use of Internet



The Bar Chart above assessed views of respondents on the site they access when on the internet. The data obtained show that majority of the respondents' access google search, social media and use the internet for academic research. While only few respondents use the internet for pornography, spamming and piracy. The low responses of respondents on whether they access pornography, are involved in piracy and spamming while on the internet is due to the sensitivity of the topic under study, however, they could be viewing pornography or involved in piracy secretly. From the chart, it can be inferred that respondents use the internet for either pleasure or academic research.

From the in-depth interview (IDI) conducted, a cyber-criminal stated that:

Basically there are many things I do on the internet but what I spend most of my time doing is on facebook, yahoo mail, chat room and piracy. I get cool money from downloading software and selling it.

In a bid to know what he uses the social network for, he stated that; I use it to send fraudulent mail to my target.

Table 4.3.2: Awareness of the Term Cyber-Crime

Awareness of Cyber-Crime	Frequency	Percentage
Yes	375	93.75
No	25	6.25
Total	400	100.0

The Table above assessed the views of respondent's awareness of the term cyber-crime. The Table shows that majority of the respondents are aware of the term cyber-crime. This implies that respondents will be capable of filling and providing adequate and useful answers/information to the questions in the questionnaire.

Also, the results from the IDI conducted shows that all the respondents interviewed are aware of the term cyber-crime as they were able to define the term. For instance one of the lecturers interviewed when asked about the definition said that:

Cyber-crime is derived from two words "cyber" and "crime". Cyber refer to any activities either sales or transaction of services in the cyber space while crime are unacceptable activities. When join together, it means all fraudulent, illicit, and unacceptable activities related to cyber.

Similarly, another lecturer aired his views as follows:

Cyber-crime is derived from 2 words cyber and crime. Cyber has to do with the World Wide Web or interconnection of computer while crimes are all illegal activities. When join together it is define as crime committed via the cyber-space.

Furthermore, another lecturer added that; its awareness is high, as most enforcing agencies and legal agencies are now aware of the issues and the tools to fight the crime.

An operator of cyber-café also agreed with the above definition and gave the definition of cyber-crime as thus:

Cyber-crime is committing crime through the internet, it does not necessarily mean it has to happen inside the cyber-café, you can have your laptop, you have your modern in your house and you commit crime; hack people's mail. That is cyber-crime.

In addition, a cyber-criminal when asked during the IDI how long he have been involved in cyber-crime stated that; I have be doing it for while, let say 4 to 5 years now.

From the findings, it can be deduced that virtually all the respondents are aware of the term cyber-crime.

Table 4.3.3: Frequency of Cyber-Crime in Tertiary Institutions in Zaria

Frequency of Occurrence	Frequency	Percentage
Frequent	197	49.25
Not frequent	173	43.25
Undecided	30	7.5
Total	400	100.0

Table 4.3.3 indicates that majority of the respondents agreed that cyber-crime is frequent in tertiary institutions in Zaria.

The IDI conducted also showed that most of the key informants agreed that cyber-crime is frequent in the study area. For instance an operator of cyber-café states that:

When my café was newly open in 2010, customers that come to browse try to beat our timing system until measures were put in place to curtail them from stealing our time. But people still come to send fraudulent mail and as you can see, we don't allow flash drive into our system.

A cyber-criminal aired his view on the frequency of cyber-crime in tertiary institutions in Zaria as follows:

Cyber-crime is frequent in Zaria but an ordinarily person wont know except when you have fallen victim and this is due to the high level of poverty and many graduates are unemployed and some have computer skill, so they will use what they have to survive”.

In addition a lecturer stated that:

Cyber-crime is any crime committed via the internet, so people watching pornography is committing crime, those people sending fraudulent e-mail that is phishing is also committing crime. And those trying to download academic materials, text books or software from the internet without paying for it are also committing crime. So you can see that everybody is involved in this crime.

However, a lecturer who was not in support of the high frequency of cyber-crime states as follows; cyber-crime is not frequent in tertiary institutions in Zaria, or can you compare its frequency with schools located in places like Lagos, Calabar, Benin or PH. From the above data obtained, it can be deduced that cyber-crime is frequent in the study area.

Table 4.3.4: Persons involved in Cyber-Crime

Persons involved Cyber-Crime	Frequency	Percentage
-------------------------------------	------------------	-------------------

Youth	346	86.5
Adult	45	11.25
Aged	9	2.25
Total	400	100.0

The data in Table 4.3.4 revealed the categories of people involved in cyber-crime. The Table shows that majority (87%) of those who are involved in cyber-crime are youths. This view is in agreement with the responses from the qualitative data. For instance, an operator of cyber-café aired his view when asked about the categories of those involved in cyber-crime as follows; young people are mostly involved in one kind of cyber-crime or the other.

Furthermore a lecturer consented to the statement that:

Cyber-crime is more common among younger people than with the older ones. This is due to the fact that the internet and PC are artifacts of the last decade. As a result of this, members of the younger generation tend to be more familiar with the technology and more active in deviant behavior.

In line with the above statements, a male youth who is involved in cyber-crime related how long he had being involved in cyber-crime as follows; I started online fraud before I entered the university, then I use to work in a café and some boys use to come to do yahoo yahoo stuff. So I learnt from them.

In contrary to the above views on the person usually involved in cyber-crime, a lecturer states that:

Cyber-crime can be committed by anybody. A thief is a thief not minding the age. Like I said earlier, people who download software illegally are thieves, so you can see people in their forty's or fifty's doing what the younger ones are doing.

From the findings, it can be deduced that most individuals who perpetrate this criminal act are youths.

Table 4.3.5: Time of Perpetration of Cyber-Crime

Time of Perpetration	Frequency	Percentage
Day	30	7.5
Night	173	43.25
Any time of the day	197	49.25
Total	400	100.0

Table 4.3.5 dwells on the time cyber-crime is being perpetrated. Finding shows that most of the respondents agree that cyber-crime can be perpetrated at any time of the day. Similarly, findings from the IDI also agree with this statement that it can be committed at anytime of the day. For instance a cyber-criminal stated that:

Cyber-criminals have mastered the use of time while committing/carrying out their criminal activities. For example in ATM fraud, when cyber-criminals discovered an account, they carry out their attacks mostly on weekends and mostly outside the state where the account is domiciled and at any time of the day.

A lecturer who also corroborated with the above statement, stated that; cyber-crime can be committed at any time of the day because it depends on the type of crime, the geographical place and time where their targets are located, all these factors are put into consideration.

A cyber-criminal when asked about the time he perpetrates the act, had this to say:

I do my things in the evening or at night when the network is better and people using the network have reduced. Take for example if I am to download a software, it will be faster at night than during the day.

It can be deduced from the above statements that cyber-crime is mostly committed at any time of the day but a cyber-criminal who is involved in piracy will commit the crime at night.

Table 4.3.6: Point/Place where Cyber-Crime is Perpetrated

Point/Place	Yes		No		Total	
	N	%	N	%	N	%
Cyber-café	323	80.8	77	19.2	400	100
At home	317	79.3	83	20.7	400	100
Private organization	206	51.5	194	48.5	400	100
Government office	94	23.5	306	76.5	400	100

Table 4.3.6 shows the perpetration points of cyber-crime. The data collected reveal that 81% of the respondents agreed that cyber crime is usually perpetrated at cyber-café while 80% said at home. This is to confirm the earlier statement made by an operator of cyber-café that with the introduction of internet modems, blackberry and smart phones cyber-crime could be committed at homes.

The qualitative data obtained supported the quantitative data. For example, a cyber-criminal has this to say when interviewed on what he used to browse or how he accessed the internet:

I have my private modem and laptop that I use to browse at home. Let me tell you, nowadays cyber-criminals don't use the café any more, they now use wireless and blackberry to access the internet and operate comfortably from their homes.

In addition, a lecturer stated when asked about the perpetrated point of cyber-crime that;

My view on the perpetrated point of the crime is the home. This is due to the fact that even ordinary Nokia C3 can browse and with the reduction in the price of MB, anybody who is interested in criminality can afford it.

It can be deduced from the findings that youths don't usually go to the cyber-café anymore; they get access to the internet with their private modem and personal computer or laptop and commit the crime without leaving their homes.

Table 4.3.7: Nomenclatures of Perpetrators of Cyber-Crime

Nomenclatures	Yes		No		Total	
	N	%	N	%	N	%
Yahoo yahoo boyz	386	96.5	14	3.5	400	100
Yahoo millionaire	202	50.5	198	49.5	400	100
Yahoo zee	161	40.3	239	59.7	400	100
Forex trade	148	37.0	252	63	400	100

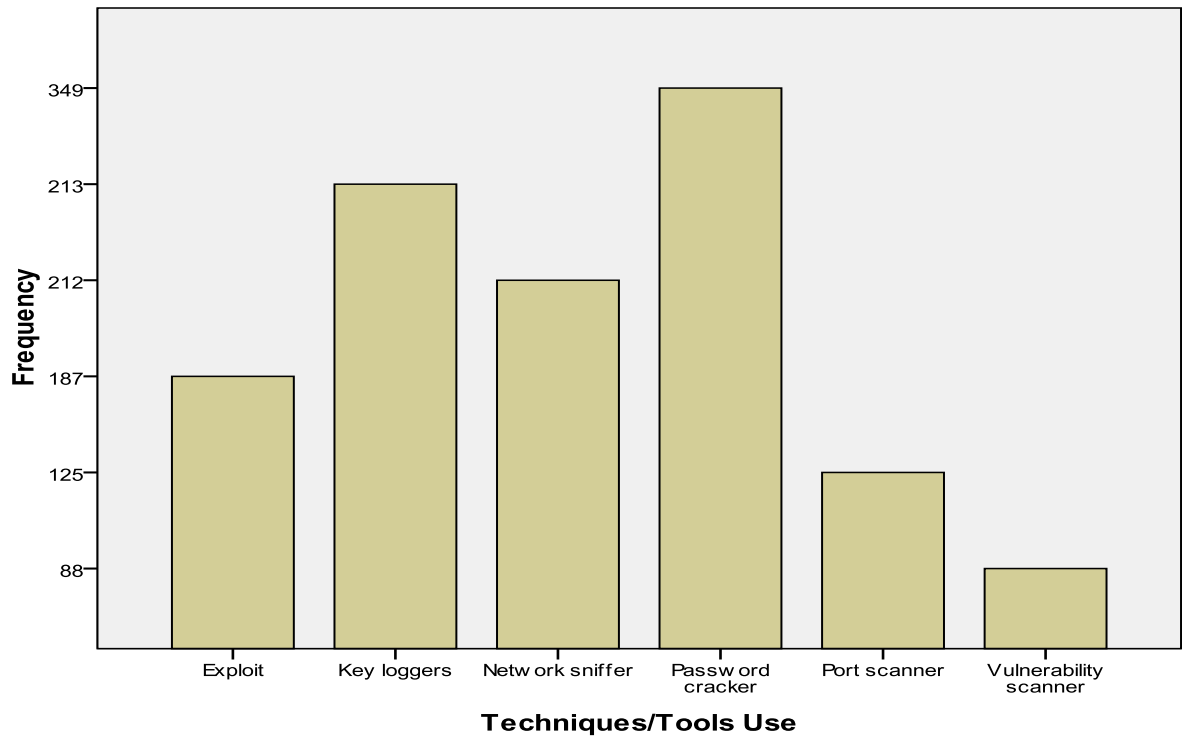
Table 4.3.7 revealed the nomenclatures that most cyber-criminals are known as or usually nicknamed. Virtually, all the respondents said that cyber-criminals are nicknamed "yahoo yahoo boyz". This implies that a large percentage of the people have heard of "yahoo yahoo boyz" and they equally know what they engaged in.

In support of the above statement that most cyber-criminals are referred to as yahoo yahoo boyz, a lecturer has this to say in the IDI conducted that:

The name yahoo yahoo boy has become a household name. It simply refers to criminals who indulge in advance fee fraud schemes or involve in internet crime. These yahoo boys enjoy status of big boys in the society and are socially recognized among their friends and

everywhere you see yahoo boys, other boys not involved in the crime will want to associate with them due to their flamboyant life style.

Figure 2: Techniques/Tools use by Cyber-Criminals



The Bar Chart above shows the respondent's views on the various techniques/tools used by cyber-criminals to perpetrate their criminal act and password cracker was discovered to be the commonest techniques used by cyber-criminals. Similarly, efforts were made using the IDI to find out more techniques/tools used by cyber criminals. The qualitative data show that there are other techniques/tools aside the aforementioned that cyber-criminals use to perpetrate their act. For instance, a lecturer said that:

There are various techniques/tools cyber-criminal use to perpetrate their act. They can use mathematical model. A mathematical model is a process where cyber-criminals sit down to design a program using Tree diagram, a statistical tools. This is then link with their

victim account and the tree diagram keeps checking and checking until it gets the combination of that victim Pin number. Then there is also the phone techniques where the cyber-criminal calls his victim to inform him/her that he/she has won a lottery and he then direct his victim to a particular ATM. He ask his victim to check the ATM that there is something called phone charge though it is suppose to be a cash transfer button but it is not written like that and he dictate a number to his victim. This number been dictated is his own personnel number and ask his victim type any amount of money and once the amount is typed, it is been deducted from the victim account number.

Another lecturer stated that:

The techniques cyber-criminal use are quite verse. We have Sniffing. Where cyber-criminal sniffs into people's passwords in order to get information that will authenticate them access into your account. Another technique is what is called Man in the Middle. Here cyber-criminals take advantages of the loopholes of an organization. When ever the victim is communicating with the organization, they also have the privileges to such information and therefore use it against the victim. There is another technique called the Honey Pot. Here the cyber-criminal create sites that are interesting to people. Take for example in this country we like free things, so cyber-criminals can create a site for free software download. When you enter these sites, they ask you to supply some information about yourself thereafter lunch their attack.

To corroborate the aforementioned, a cyber-criminal has this to say:

There are several types of techniques I know cyber-criminals use to get their victim, it all depends on individual skills and talent. For example, some of us create websites that appear legitimate but in reality are scam designed to defraud or obtain information that can be used to commit further economic crimes.

Similarly another cyber-criminal gave his own view on the techniques used by cyber-criminals:

In credit card or ATM fraud, I know some of us have powerful software which could assist to access all the account numbers of people that have come to a particular ATM to withdraw. Once they scrutinize the account number and see the one that has big money in it, they then use another type of software to transferring the money into their own

account instantly. Sometimes, we use social network such as facebook and other chatting network to deceive people to give out their personal data or information.

When further probe on the type of technique he use for software piracy, he stated as follows:

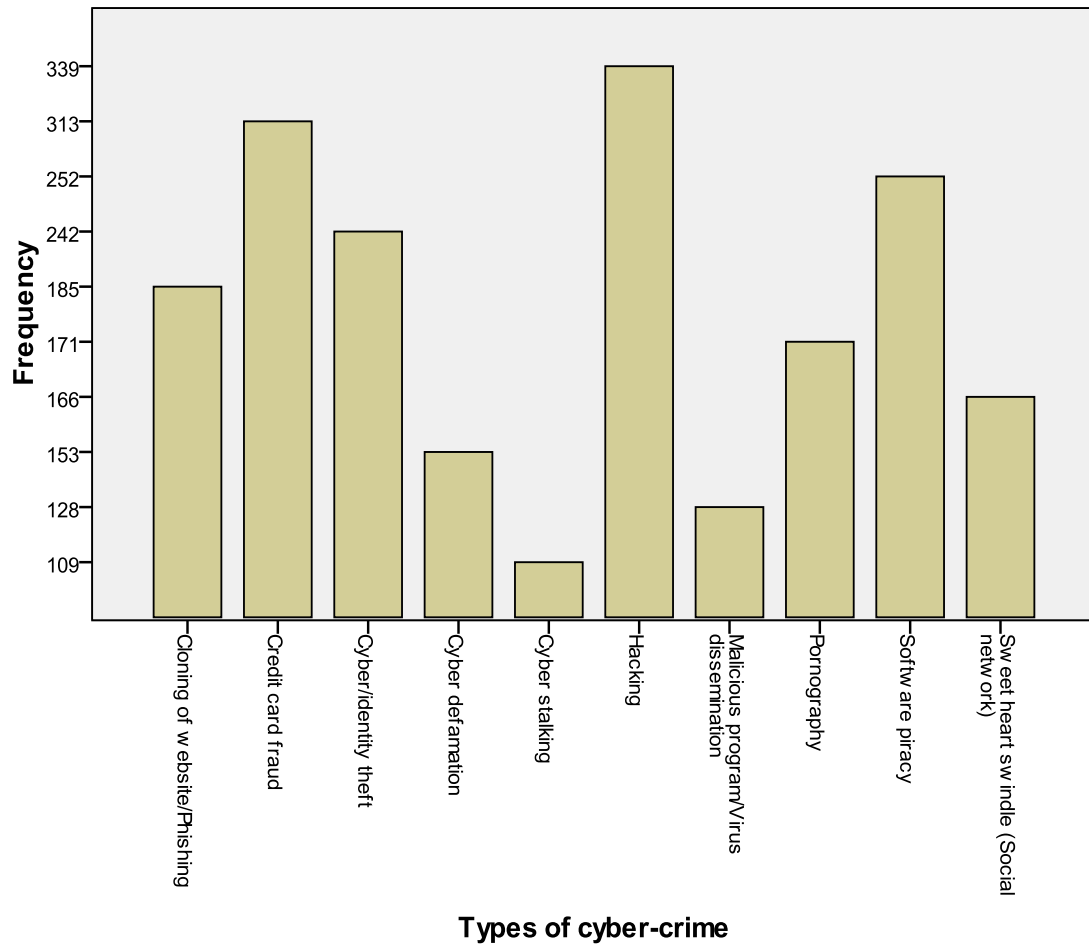
I use SQL injection to download software. Since most of the license keys to the software are usually kept in a data base, I usually write series of code that usually go to the data base to fetch the keys and I download it to my system and I use the key instantly on the software. I also use key recorder and password reviler to get the key to software too.

Concerning how they get their proceeds from their illicit act, a lecturer stated that cyber-criminals get their proceeds from any of the followings means; domiciliary account, money gram or western union. From the above, it implies that cyber-criminals use the following techniques; password crackers, key loggers, mathematical model, SQL injection, man in the middle, creating of illegal web sites, honey pot and kernel level rootkits to get their victims and they usually get their proceeds from the above mentioned means.

4.4 TYPES OF CYBER-CRIME

This section identified the types of cyber-crime that is perpetrated in tertiary institutions in Zaria. This is represented in the Bar Chart below.

Figure 3: Types of Cyber-Crime



The Bar Chart above reveals that majority of the respondents are of the view that hacking, credit card frauds and software piracy are the most common type of cyber-crime perpetrated in tertiary institutions in Zaria. In addition to the above, respondents from the quantitative data identified other types of cyber-crimes aside the listed once that are perpetrated in the study area such as alteration or disclosure of data, trafficking of passwords and credit card number, lottery, educational scam where students only pay half of their tuition fees and stealing of direct TV signals by modifying the card that goes into the satellite receivers.

Findings from the IDI also identified other types of cyber-crime common in the study area. For instance, a lecturer states that; the common types of cyber-crime in tertiary institutions in Zaria are pin fraud, cheque fraud, theft of identity, phishing and economic fraud.

Similarly a cyber-criminal when asked during the IDI to identify the type of cyber-crime he indulges in submits that:

I am into phishing and the use of social network to get my maga. What I do mainly is to pretend as an imposter via online dating. I looked for the profile of people that is male and female that lives outside the countries. I always posed to them as a single female looking for a male partner or as big man who needed a wife or tell them stories on how my wife disappointed me and took away my property and children or as a widow. All this is polished in a pitiable way with some pictures to even convince them whenever I'm chatting with them. From there I begin to play my pranks.

Another cyber-criminal when asked on the type of cyber-crime he indulges in states that; basically am into software piracy and hacking.

The findings therefore, shows that credit card fraud, hacking, software piracy, phishing and the use of social network are the major types of cyber-crime that are common and being perpetrated in Zaria.

4.5 SOCIAL ATTRIBUTES OF CYBER-CRIMINALS

In this section, an attempt was made to discuss the social attributes of cyber-criminals. It covers areas such as the age, sex, religion, educational background amongst others of cyber-criminals.

Table 4.5.1: Sighting of Cyber-Criminals

Sighting of Cyber-Criminal	Frequency	Percentage
Yes	240	60.0
No	160	40.0

Total	400	100.0
--------------	------------	--------------

Table 4.5.1 is on respondents views if they have seen cyber-criminals. Findings showed that (60%) of respondents stated that they have seen cyber-criminals. Similarly, from the IDI conducted all the key informants interviewed submitted to have seen cyber-criminals and few of the key informants admitted to have interacted with cyber-criminals. For instance, a lecturer when asked if he has seen cyber-criminals stated that:

I did my Industrial Training (IT) with a cyber café in Bauchi in 2006. During my stay there, cyber-criminals used to come for overnight browsing which I was in charge of night browsing section then. When they come, because they are aware that I know what they are doing, they used to ask me for one assistance or the other and sometimes find me some stipends. They even asked me sometimes to get them some customer's ATM Pin, account numbers and banks which I declined because then customers use to come to our cyber-café to give their banks detail when doing some certain transactions.

Another lecturer stated that; I have come across three cyber-criminals in the line of my duty and due to the nature of my profession, I even interacted with them.

An operator of cyber-café aired his views as to whether he has sighted cyber-criminals as follows:

Some individual (cyber-criminals) do come to our café to tamper/disable our café timer which will give them unlimited access to the internet. Once we discover this, we warn them and if they repeat such, we don't allow them come into our café again.

To corroborate the above statement made by an operator of cyber-cafe, another operator of cyber-café stated that:

Those cyber-criminals that come to our café trying to bypass our café timer, when caught, they were only warned but not handed over to the police for prosecution.

From the above, it implies that cyber-criminals have been seen by a significant number of people. With this, respondents were able to give detailed description on the social attributes of cyber-criminals.

Table 4.5.2: Friends who engage in Cyber-Crime

Friends who engage in Cyber-Criminal	Frequency	Percentage
Yes	50	12.5
No	350	87.5
Total	400	100.0

Table 4.5.2 shows the views of respondents if they have cyber-criminals as friends. Finding shows that majority of respondents said they don't have cyber-criminals as friends.

From the IDI conducted, a lecturer when asked whether he has friends who engage in cyber-crime states that:

When I was a student in the University, I use to have friends who indulge in cyber-crime but it have been long I heard from them. So I can't tell if they still do it or not. But like I said earlier, in the course of my duty, I have interacted with them and they are very intelligent and smart people.

Another lecturer also aired his view as to whether he has friends who indulged in cyber-crime as follows:

Like I said earlier, I did my IT in a cyber-café, then I have quite a number of guys who do this stuff. But you know it's being long so I don't even know if they still do it or not. I can't even say where they reside now. Why they were my friends then was because I was the one in charge of the night browsing and they always come at night then.

Table 4.5.3: Social Attributes of Cyber-Criminals

Views	Frequency	Percentage
Age		
18-30	351	87.7
31-40	44	11
41 above	5	1.3
Undecided	0	0.0
Total	400	100.0
Sex		
Male	355	88.75
Female	19	4.75
Both	26	6.5
Total	400	100.0
Religion		
Islam	65	16.3
Christianity	117	29.3
Traditional	40	10.0

Any Religion	178	44.4
Total	400	100.0
Individual Qualification		
Primary Education	13	3.25
NCE	17	4.25
Polytechnic	49	12.25
University	239	59.75
Others (computer education, master degree)	82	20.5
Total	400	100.0
Marital status of parent		
Married	242	60.5
Divorced	79	19.7
Widow	22	5.5
Undecided	57	14.3
Total	400	100.0

The data in Table 4.5.3 show respondents perception on the socio attributes of cyber-criminals.

The data reveal that majority (88%) of the respondents were of the view that those individuals who are involved in cyber-crime are within the ages of 18-30years.

Findings from the qualitative data corroborated with the above result on the age of cyber-criminals as all key informants interviewed agreed that cyber-criminals are mostly teenagers. For example, a lecturer said that:

Cyber criminal are mostly between the ages of 20yrs and above. You can only cut the age lower but not upper because you can see a good cyber-criminal at the age of 60yrs who will claim to have been doing it right from his youth age but most of the people I met are in their late 20's.

Another lecturer also argued in the same vein that:

Cyber-criminals are mostly youths between the ages of 20-35yrs. This may be due to the early exposure of the young ones to the activities on the internet without proper guidance. I think that is the reason why cyber-crime is more common among that age bracket.

The above statement was also supported by an operator of cyber-cafe who said that:

In general I would say that those involved in cyber-crime are much more inclined to be younger than older. Though, we have seen people in their 30's and 40's indulging in the act. But all in all I would say that younger people are more adapt at this simply from the nature of their growing up with it.

From the above statement, it can be deduced that cyber criminals are individuals who are mostly within the age bracket of 18-30years.

The Table also discloses the sex of cyber-criminals. It was discovered that the male youths (89%) involved more in cyber-crimes. Findings from IDI also agreed to the data obtained from the table.

For instance, a lecturer states that:

Those involved in cyber-crime are mostly male. And based on citation from books, journals as well as film, they are mostly male, may be the female folks are not interested in such act. I can say the ratio of male to female in cyber-crime is 75:25.

Another lecturer corroborated the above statement that; most of the cyber-criminals are male. Basically, it is a male issue because they do it in order to get wealth, build houses, buy cars and get beautiful ladies.

However, the key informants were further probe in order to find out if they have seen some female(s) do perpetrating the act too. In line with this, most key informants submitted that it is basically a male issue with only a little percentage of female involve in the crime. For instance, an operator of cyber-café had this to say:

I will say 99% of cyber-criminal are guys. A lot of guys are involved in this act. Though I once came across a very powerful computer programmer and she was a lady. If she decides to use her knowledge negatively, she will be a good cyber-criminal.

Similarly, a lecturer also stated that: females too are involved in cyber-crime but the ratio is very small when compared to the male. You can hardly see a female cyber-criminal in Nigeria.

Table 4.5.3 also shows the religion background of cyber-criminals. The study reveals that cyber-criminals could be from any religion which represents (45%) of the total views of respondents. The qualitative data also agreed with the data obtained from the table. For instance, a lecturer stated that:

You cannot easy identify them by religion. And religion does not come to play in one been a cyber-criminal because no religion preaches criminality. It all depends on the individual and the company in which he follows.

Also an operator of cyber-café corroborates the above statement that a cyber-criminal could be from any religion.

Finally, a cyber-criminal when asked of his religion, he stated that he has a Christian. When he was further asked about the religion background of other cyber-criminals, he stated that; cyber-criminals could be from any religion, cyber-crime is not limited or restricted to one religion. From the above data, it can therefore be deduced that religion is not a barrier to cyber-crime.

The Table also revealed the educational background of cyber-criminals. Findings show that majority (60%) of the youths who engage in cyber-crime are university students. However, key informants in the IDI did not agreed to the statistics obtained in table 4.5.3 on the educational

qualification of cyber-criminals. They are of the views that cyber-criminals must have possessed one form of educational qualification or the other. For instance an operator of cyber-café states that:

You don't need to have a university degree before you can commit cyber-crime. In fact cyber-crime is not committed by dull people. You must be intelligent and smart and most youths that are involve in this crime are found in any kind of tertiary institution we have in Nigeria.

Similarly, a lecturer also corroborated the above statement that:

Cyber-criminals can be in any tertiary institution, they could as well be in secondary school depending on the individual exposure to the technology. What I believe is that cyber-criminals are not only smart people who have the skill to manipulate and alter technology to fit their needs, they are also smart enough to understand the human element and manipulate human nature to fit their needs.

From both qualitative and quantitative data, it can be deduced that cyber-criminals can be in any of the tertiary institutions listed above and must possess additional attributes such as smartness and intelligence in order to cheat and defraud innocent individuals. It can also be deduced that it is not easy for low level young individuals with low intelligence quotient to be involved in cyber crimes.

In addition, the Table also reveals that a significant number of the respondents (61%) were of the views that most cyber-criminals are from married home. Similarly, the data obtained from the quantitative data was supported by the statement made by a cyber-criminal when asked about the marital status of his parent, he said that; my parents are still married and they live together.

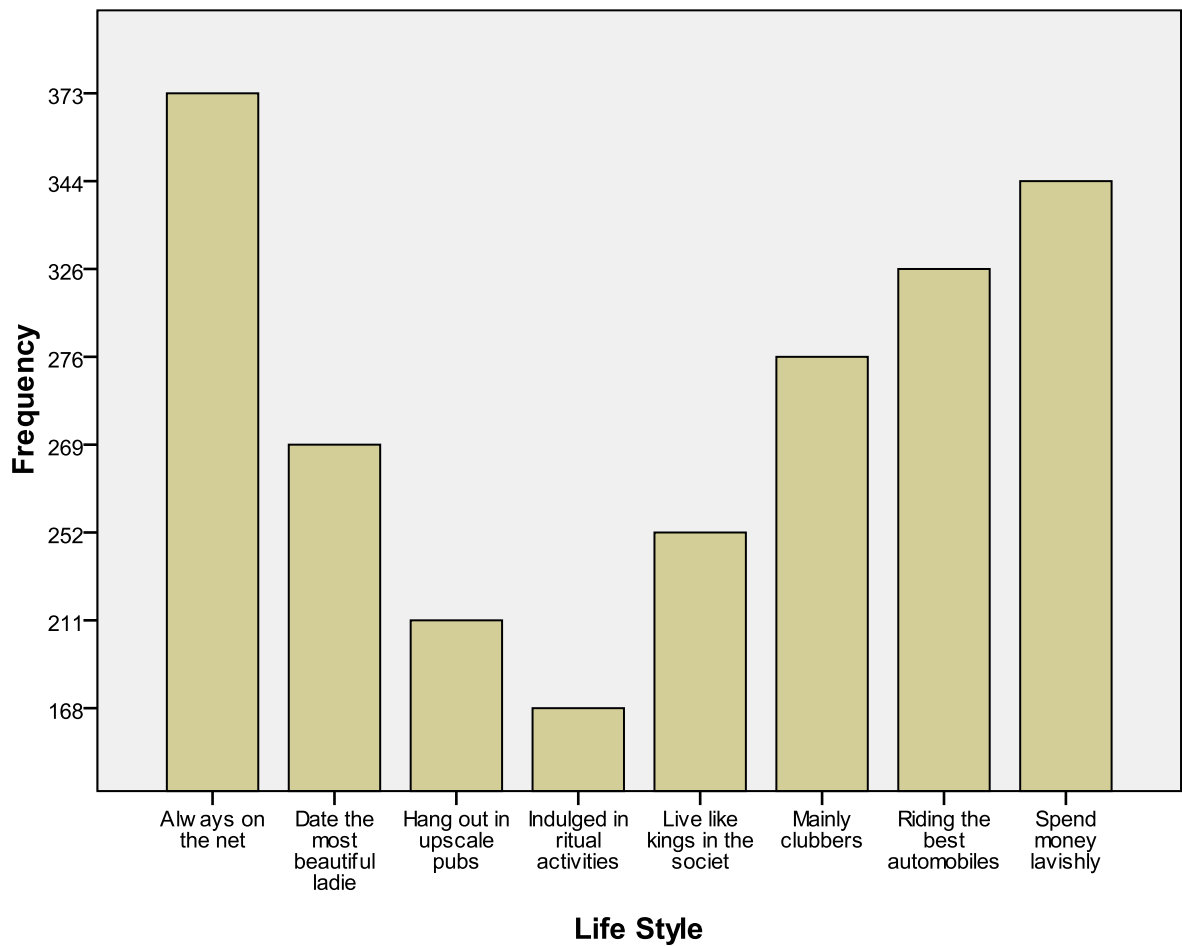
However, some of the respondents in IDI have a contrary view on the parent marital status of cyber-criminals. For instance, a lecturer stated that:

The involvement of individuals in cyber-crime is not a function of the marital or socio-economic status of their parents. Individuals from both rich and poor homes or monogamy and polygamy or broken and not broken homes all engage in the crime.

Another lecturer says that:

In Nigeria, youths who are involved in cyber-crime does not need to come from a broken or unbroken home. Reports from EFCC on those cyber-criminals caught and sanctioned indicates that they are either from broken or unbroken home and also findings from previous research on this topic indicates that parents have abdicated their parental roles in pursuit for money leaving them to develop anti-social attitude.

Figure 4: Life Style of Cyber-Criminals



Data in the Bar Chart presented respondents views on the life styles cyber-criminals possess. The result shows that majority of the respondents are of the view that cyber-criminals are always on the internet and spend money lavishly amongst others listed above.

In support of the above life style of cyber-criminals, a lecturer in the IDI conducted stated that:

Some of them when they hit it big, they do good thing for themselves and their parent. They ride good cars, dress flashy, always attending clubs. Those I knew then in the

university were using good cars. Then Toyota camry and this baby boy were expensive not now that it is pure water.

In addition, a cyber-criminal when asked what he does with the proceeds of the money he receives from the criminal act stated that:

What I do mainly with the money I get from the sales of the software I get from the internet is to assist myself in school, have more money to subscribe for airtime and I also spend for my siblings and girlfriends.

When further asked if he indulge in ritual activities states that:

I don't do such, however I know that some of us do such by consulting spiritualists and herbalist in order to continue to be successful and also to assist them charm their victims in order to dance to their tune.

From the above, it can be inferred that cyber-criminals have a flamboyant lifestyle that is quite different from others individuals in the society.

4.6 CAUSES OF CYBER-CRIME

In this section, an attempt was made to identify the causes and motivating factors that are responsible for the involvement of individuals in cyber-crime. Respondents were asked to state the motivating factors while the causes of cyber-crime was broadly given and respondents were asked to rate them based on a scale given.

The motivating factors that encourage or drive individuals into cyber-crime according to respondents vary and the different factors are money/financial gain, recognition/fame, low rate of conviction or even being caught, easy to perpetrate, intellectual pursuit, frustration, revenge, display of wealth by corrupt politicians and yahoo yahoo boys, laziness, un-satisfaction from what they earn, lack of good moral upbringing from parents and guardians.

The qualitative data gave an explicit explanation of the motivating factors. A lecturer stated that:

Some one may have grudges with an organization. A new organization can come and take away his market and you don't feel happy about it and you try to create something that will render that service that organization is producing ineffective. Take for example there are people that design program and anti virus to make money e.g AVG and Avast. One of these companies could develop virus that the other company anti-virus software won't be capable of handling and tend to make that anti virus ineffective. Then another motivating factor is the tremendous success rate of the Yahoo Boys from their illegal act and not been caught by the law enforcement agencies, this will only serves to encourage others. Others motivating factors include excitement to succeed, get-rich syndrome, vengeance and sometimes sabotage.

Another lecturer says that:

The motivating factor for cyber-criminals is that they are been reinforced for their behavior by their family members, relations and friends and not been punished for such act. For example some of these boys after hitting it big build impressive homes and buys cars for their parents and themselves and the parent won't ask where the money is coming from.

In addition, another lecturer who also expresses his view on the motivating factors states that:

Some of them want to test their acquired knowledge; some do it as a hobby while others see it as fun. Others try to imitate other rich guys in the society and finally the A and A factor. A and A means availability and accessibility. By availability you have the model and

airtime while accessibility means the internet is not monopolized. One is free to enter any site once you have enough airtime.

Furthermore an operator of cyber-café said that:

The motivating factors varies, but I think that inadequate legislation, financial benefits, low costs of executing the crime, low probability of being caught and prosecuted (due to weak laws and enforcement mechanisms) and the level of stigmatization of cyber-criminals has not been so great.

One of the cyber-criminal states that:

When asked what motivated him into such criminal act:

You have seen our Nigerian politicians; you see the way they celebrate wealth, this serves as a motivator for my involvement and other youths in cyber crime. The Nigerian society celebrates wealth without questioning the source of the money. Politicians caught defrauding the state become members of committees of the state and are given national awards like what we just experienced recently. In churches and mosques, corrupt individuals are invited to launch building projects and hold esteemed positions so why won't I find a way to survive from the economic hardship so that they can also call my name.

Finally, another cyber-criminal aired his view on why he indulged in cyber-crime as follows:

The main reason is those software which I love to use are mostly expensive and I do not have the resources to cope with buying the original software, instead I attempt to hack the software so that I can use it at my own discretion and even sell it too to make some money. Then in our peer group, we use it as a form of getting reputation for example, if one successfully crack a software, you gain some respect from our friends.

From the above, it can be deduced that the quest for quick luxurious comfort, easy to perpetrate, low chance of cyber-criminals being caught and even lower chances of been convicted by law

enforcement agencies, vengeance, sabotage, reinforcement of criminal behavior by family members, lack of resources to purchase original software, gain reputation among peer groups, pleasure and inadequate legislation are the motivating factors for the engagement of individuals in cyber-crime.

Table 4.6.1: Causes of Cyber-Crime

Views	Agreed		Undecided		Disagreed		Total	
	N	%	N	%	N	%	N	%
Unemployment	375	93.75	15	3.75	10	2.5	400	100
Poverty	346	86.5	20	5.0	34	8.5	400	100
Peer group influence	345	86.25	41	10.25	14	3.5	400	100
Defective socialization	265	66.25	89	22.25	46	11.5	400	100
Weak laws	297	74.25	38	9.5	65	16.25	400	100
Corruption	364	91	23	5.75	13	3.25	400	100
Easy accessibility to internet	302	75.5	30	7.5	68	17	400	100

Table 4.6.1 measures respondent's views on the causes of cyber-crime in the study area. The Table showed that virtually all the respondents agreed that unemployment is a causal factor of cyber-crime in the study area. This view is in agreement with the responses from the IDI conducted. For instance, a lecturer in the IDI aired his view as follows:

I will say lack of job/employment is causing a lot of problem in the society. The employment rate in the country is degenerating on daily basis and many institutions are turning out large number of graduates yearly. Take for example someone who is a graduate, who is seeking for job and it is not forth coming, so he is encourage/influence by either his peers or the economic hardship to engage in it in order to survive.

Another lecturer states that; with the increase in the rate of unemployment in the country, cyber-crime serves as a major source of employment and survival especially among the youths that have the computer skills. In addition, a cyber-criminal when asked about the causes of cyber-crime in the study area stated that; poverty and unemployment are the major causes of cyber-crime in the society and the only means of surviving is through been creative. Therefore, from the above, it can be inferred that unemployment is a cause of cyber-crime in the Zaria.

Also from the Table, 87% of respondents agreed that poverty is a major cause of cyber-crime in Zaria. , the view of a key informant in the IDI supported the quantitative data that poverty is a major cause of cyber-crime. For instance, an operator of cyber-café stated that:

Poverty is the main cause of cyber-crime in the society. Poverty is on the increase daily and there are many individuals on the street who can not afford three square meal in a day or let me say living below economy standard. So there involvement in cyber-crime may, therefore, be linked to survival and to cope with the economic hardship which is as a result of poverty.

The Table further shows that the respondents were of the view that peer group influence is a contributing factor to the causes of cyber-crime in Zaria. The IDI conducted gave a better explanation on peer group influence as a causal factor of cyber-crime. For instance, a lecturer stated that:

Many youths will continue to be involved in cyber-crime or yahoo yahoo due to the fact that many of their friends are involved in the crime too. The crime has eaten so deep into the social life of our youths especially students that most students now concentrate more on how to make money through the net than focusing on their academic work.

A cyber-criminal when asked how he was initiated into the crime stated that; I was introduced to the crime before I entered the university by my friends who are expert in the crime. From the above, it can be deduced that peer group influence is a cause of cyber-crime in the study area.

The Table also revealed that the respondents were of the views that defective socialization and weak laws/absence of existing cyber-crime law are the causes of cyber-crime in tertiary institutions in Zaria.

The IDI conducted also supported the data in the table on weak laws as a causal factor of cyber-crime. For instance, a lecturer stated that:

Yes it is a factor because the bill that will specify punishments for all types of cybercrimes has not been enacted into law by the National Assembly. The absence automatically serves as an opportunity for cyber-criminals to perpetrate their criminal act.

The findings also shows that majority of the respondents (91%) agreed that corruption is another factor causing cyber-crime. The Table finally showed that 75% of the respondents were of the view that easy accessibility to the internet is a causal factor of cyber-crime. It is therefore deduced from the above; that poverty, unemployment, peer group influence, defective socialization, weak laws/absence of existing law, corruption and easy accessibility to the internet are the causes of cyber-crime in tertiary institutions in Zaria.

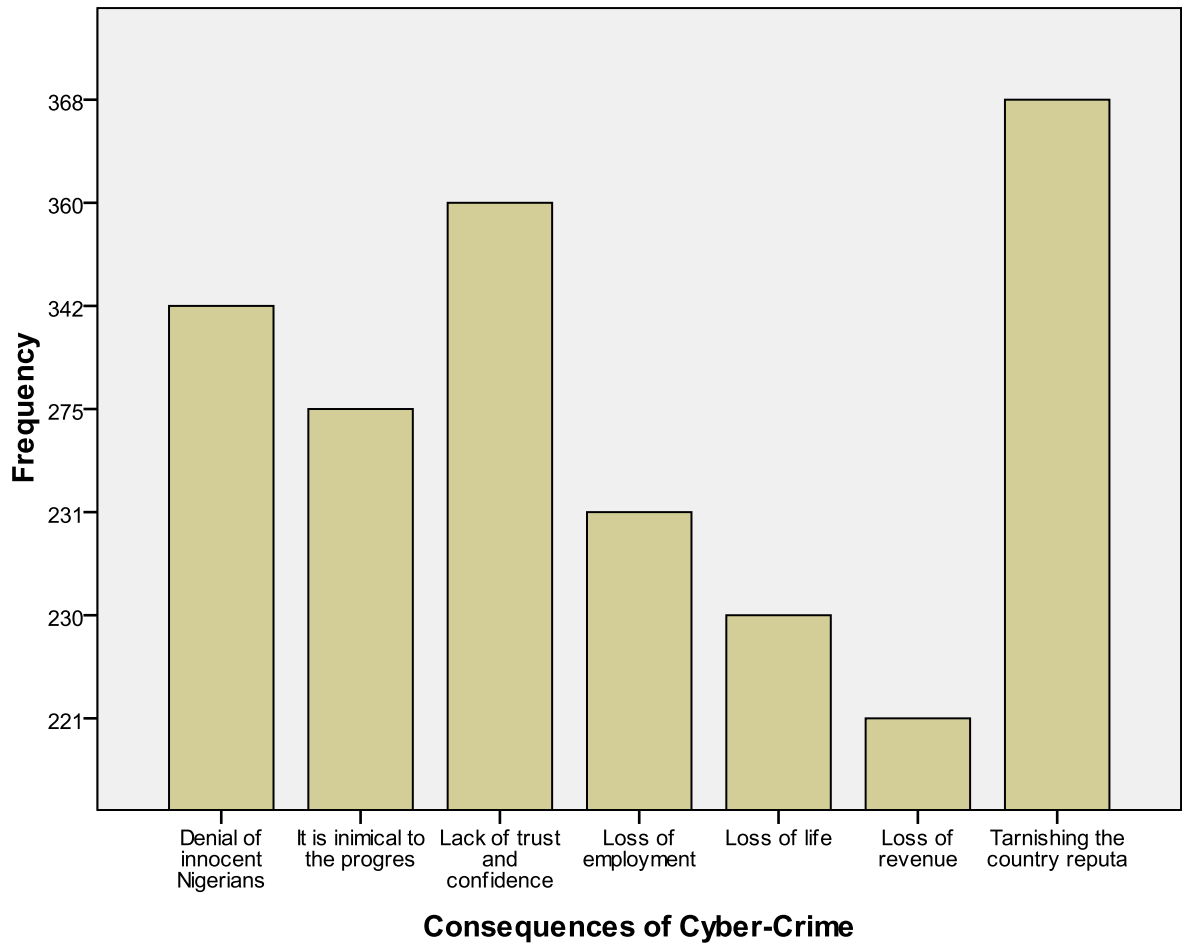
4.7 CONSEQUENCES OF CYBER-CRIME

This section delved into the consequences of cyber-crime. The consequences discussed are loss of life, tarnishing the country's image internationally, loss of revenue amongst others.

Respondents views on the Consequences of Cyber-Crime

Respondents were asked if cyber-crime has negative consequences in the study area. The result obtained from both qualitative and quantitative data showed that virtually all the respondents agreed that cyber-crime has negative consequences.

Figure 5: Consequences of Cyber-Crime



The Bar Chart above shows the negative consequences cyber-crime has in the study area. The findings revealed that majority of the respondents are of the view that cyber-crime will tarnish the

country's reputation internationally. Lack of trust and confidence which is currently hindering profitable transaction was also examined as a consequence of cyber-crime and the findings showed that most of the respondents agreed that it will hinder profitable transaction. The Table further reveals that the respondents were of the view that cyber-crime will lead to loss of life and revenue.

The IDI conducted reveals other negative consequences of cyber-crime as follows. A lecturer stated that:

Cyber-crime creates a bad image for Nigeria and this have earned Nigeria is present ranking/rating in Transparency International where Nigeria is been listed as one of the most corrupt nation in the world. Another consequence of cyber-crime is that it will drive away investors because due to the fact that most things are done electronically and if someone can attack your data base, then he have everything about you at his disposal.

Another lecturer aired his view on the consequences of cyber-crime as follows:

Cyber-crime will bring about bad international reputation and will lead to rejection and ostracization by developed countries. It will also drive away investors. For example if an investor knows that higher percentages of the workforce are criminals, it will scare him away. Another consequence is that if most youths are involved in this type of crime, there is no future for this country and finally it will lead to distrust from developed country.

One of the operators of cyber-café interviewed also states that:

Yes it has negative consequences, plenty negative consequences. Take for instance, if a white man comes to Nigeria to survey in order to invest and he discovered or he is receiving fraudulent mail from different people, he won't invest in the country again.

Nevertheless, a cyber-criminal interviewed had this to say on the consequences of cyber-crime:

For sure cyber-crime has negative consequence. Or what bad thing that does not have negative effect on the country. Cyber-crime threatens foreign investment as well as misrepresents the country among other nations as corrupt. It will also lead to stigmatization of business men and women and they will face certain barriers when carrying out legitimate businesses.

However, a cyber-criminal was of the view that cyber-crime plays a dual role in the society when asked about the consequences of the crime. He states as follows:

Yes it has negative consequences and among it is that it drive away investors. But not minding the negative consequences it has on the country, it is a way of getting connected and being rated well in the family, school and society, that is if you succeed. It is also a way for survival due to the high rate of youth unemployment and high poverty rate in the country. Take for example now, the money I get from the sales of software I download free from the net, I use it to take care of my needs. These days, when you graduate, you will not find a job even after you has spent so much to obtain a good certificate.

From the above, it can be deduced that cyber-crime has negative consequences on the economy, however, it also serves as a means of survival for those who individual who indulged in it.

4.8 SOLUTION TO CYBER-CRIME

This part of the chapter is on solution to cyber-crime. Various options were given and respondents were asked to tick the most appropriate solution to the menace.

Table 4.8.1: Respondents View whether Cyber-Crime can be Controlled

Views	Frequency	Percentage
Yes	375	93.75
No	25	6.25

Total	400	100.0
--------------	------------	--------------

Table 4.8.1 shows the respondents views as to whether cyber-crime could be control or minimized in the society. The findings show that an overwhelming number of the respondents are of the views that cyber-crime can be controlled or minimized in the society. In support of the above view, all the key informants in the IDI agreed that cyber-crime can be controlled and minimized to the barest minimum. For instance, a lecturer says that; it is not possible to eliminate cyber-crime totally from the cyber space but it is quite possible to check them.

Table 4.8.2: Solutions to Cyber-Crime

Solution to Cyber-Crime	Frequency	Percent
Empowerment of youth	355	88.7
Enlighten young ones about the consequences of such act under the law	333	83.3
Government regular engagement with IT industries to develop strategies that can prevent and curtail cyber-crime	319	79.7
Zero tolerance to corruption	315	78.7
Arrest and immediate prosecution of cyber-criminals	294	73.5
Report to the police or other concerned authorities anyone we might suspect of engaging in cyber-crime	293	73.3
Redefine our ethical standards	281	70.3
Introduce cyber-crime as a course in the curriculum of secondary school students	260	65.0

Table 4.8.2 shows the respondents views on the possible solution to curtail the menace. The finding shows that majority of respondents were of the view that the empowerment of the youths will go a long way in providing a lasting solution to cyber-crime in the society. This view was also supported in the IDI conducted. For instance, a cyber-criminal states that; government should

create jobs so that youths will gain employment and use their knowledge to do good instead of bad. In addition, a lecturer stated that:

Throwing money on measures to curb cyber-crime is not addressing the issues of cyber-crime, the best solution is for government and foreign investors to invest in the economy. Adequate investment will lead to creation of jobs and basic amenities which will in turn make everybody engaged and this will serve as a solution to the crime.

Finally, an operator of cyber-cafe also aired his view on the empowerment of youths as follows:

Government and multinational companies need to create more jobs for the masses. This job creation will redirect the energy and time Nigerians used to commit all form of crime towards productivity.

The Table also shows that (83%) of the respondents were of the view that youths should be enlighten about the consequences of cyber-crime under the law. This can be achieved through massive publication on posters, placards, television and other mass media means. The qualitative data also agreed with the quantitative data. For instance, an operator of cyber-café states that:

Many of the problems caused by cyber criminals can be avoided by creating a forum to educate people on the danger and effects of this kind of crime on the economy. It is also important that individual users of the internet are educated too on the risk of disclosing their personnel information on the net and how to be secured otherwise they are going to do stupid things, things that will deliberately put them in a mess.

Another operator of cyber-café stated that:

The first thing to solve the problem of cyber-crime is orientation. There is need to orientate the public on the usage of the computer and internet before they jump up, buy modem and start browsing.

Finally, a lecturer says that; the public must be educated about the problems, risks and solutions of cyber-crime.

Furthermore, the Table shows that 80% of respondents were of the view that government regular engagement with IT industry to develop strategies that can help prevent and curtail cyber-crime would assist in curbing the menace. This view was in agreement with the responses from the IDI conducted. For instance, a lecturer stated that:

Cyber crime perpetrators will continue developing and upgrading their skills and techniques on daily basis in order to stay ahead of the law enforcement agencies. Therefore, security measures such as the introduction of biometrics using the faces, eyes, finger print in all sector of the economy will mitigate cyber-crime in the society.

The Table also revealed that 79% of the respondents were of the view that zero tolerance to corruption by all will mitigate cyber-crime in the society. This view was supported in the IDI, for instance, a lecturer stated that:

In Nigeria, integrity and honesty are despised and everybody have embrace corruption, the best way forward for our country is for corruption to be shun at all level and all should uphold honesty and truthfulness.

In addition, a cyber-criminal was of the view that:

Government officials especially those holding key post should live by example. They should stop stealing public funds because the money they steal they use it to oppress the masses. Those government officials who embezzle public funds should be severally sanctioned. By so doing, everybody will know that nobody is above the law.

Nevertheless, the findings also showed that 74% of the respondents were of the view that the arrest and immediate prosecution of cyber-criminals will checkmate cyber-crime in the society. This solution to cyber-crime was supported in the IDI conducted. For instance, a cyber-criminal stated that:

I think the punishment and number of arrests should certainly be increased. There are many people outside there doing it and there is need to put a higher level of fear to them over what will happen if and when they get caught. Also their assets should also be confiscated by government.

The Table reveals that 73% of respondents supported the view of reporting to the police or other law enforcement agencies anyone they might suspect being a cyber-criminal as a possible solution to cyber-crime. Findings from the IDI also supported the view. For instance, a lecturer had this to say:

Cyber-criminals hide behind the fact that when they commit such act, it leaves no traces as to the actual identity of the perpetrators, but we know when someone around us is involved in cyber-crime because of the lifestyle and background of such person. If we can build the courage and disregards sentiment by reporting to the police then cyber-criminals and even all criminals won't have a hiding place in the society.

Another lecturer supported the above view, he stated that;

If everybody is ready to report to the police or other concerned authorities anyone we might suspect of engaging in cyber-crime, then we have won the battle because those criminals living in our neighbourhood will be picked one by one by law enforcement agent and they will be prosecuted as such. Take for example, the banks report any suspicious deposit, neighbour report unexplained wealth, family bring out their wards who are engaged in any criminal activities like that like that, tell me where will they hide.

Similarly, an operator of cyber-cafe when asked if reporting to law enforcement agencies will serve as a solution to the menace states that:

Yes it will and to add to it, there is need for everybody has to come together in order to provide a lasting solution to the crime. Parents should monitor what there children do on the internet since those involved in this crime are still be under the guide of their parents. Then religious groups/organizations also have their roles to play. They should preach that there is no way crime will help them become great in life. Then as individual, my advice for them is that they should have conscience.

One can therefore, deduced that reporting to law enforcement agencies any one we might suspect to be involved in cyber-crime will reduce the crime in the society because once the neighbors and everyone within the neighborhood are watching what is going on; it will send warning messages to cyber-criminals that the neighbourhood will report to law enforcement agencies any dubious act.

The result in the Table also revealed that 73% of respondents were of the view that the redefinition of our ethical standard from wealth at all cost to other cherished values will assist to control the menace. In the IDI conducted, a lecturer who is in support of the above viewed stated that:

There is total disregard for rules and a non conformist is more valued in Nigeria than a conformist who has not achieved much in life. We always want to achieve success at all cost not minding the means in which it is achieved. There is need for a redefinition of our value system.

Another lecturer was of the view that:

The society encourages people to get rich quick by any means and it accommodates them without asking questions. This is one reason why individuals take into crime because

nobody will question the source of their wealth. Until we start asking and challenging the source of individual wealth before we can get a way forward in Nigeria.

A cyber-café operator was of the view on the redefinition of our ethical standard as follows:

Leadership at all levels in Nigeria has failed the masses by their corrupt practices and this act will not promote any positive values for youths coming behind instead it will translate into social vices. There is real need to shift or redirect our value system.

Finally, a cyber-criminal aired his view on the redefinition of ethical standard as follows:

Yes there is need to redefine our value system because if you are not successful, the society look down on you even if you have a degree and the parents are also to be blame too. Some of them compare their children with other successful ones even when they know the sources of such wealth. And the parent of those one too will refuse to confront their children who come home with expensive cars and other expensive materials, even when they know such children are unemployed.

When further probed whether his parent are aware of his involvement in cyber-crime, stated as follows; no they are not aware but they know that am living above what they give me monthly and I hardly trouble them for my needs. I never hit am big that is why they never suspect me.

Finally findings from the Table also shows that 65% of respondents were of the view that cyber-crime should be introduced as a course in the curriculum of secondary school students. The IDI conducted also supported the data in the table. For instance a lecturer stated that:

Yes I support the idea of introducing it as a course in secondary school. This will catch them young and it will also be use as a means to enlighten the young ones on how cyber-crimes are committed, the consequences of such actions under law and the pain they cause others by committing cybercrimes amongst other.

An operator of cyber-cafe also supported the view, he states that; this will assist them know the consequences of being a cyber-criminal and also teach them the ethical conduct of using the internet. However, a lecturer did not support the idea of introducing cyber-crime as a course. He aired his view as follows:

Introducing the course has little or no effect on the solution to cyber-crime at the moment. Corruption has eaten so deep into the minds of all Nigerians and it is only when corruption is addressed that the system will work well. Everybody is looking for what he/she will gain and not how to make the system work.

From both qualitative and quantitative data, it can be deduced that cyber-crime can be reduced to its barest minimum if the government empower the youths by creating jobs, everybody shun corruption, redefinition of our ethical values, report cyber-criminals within our neighbourhood to the police, parents should train their children with good morals and value and confront their children who come home with expensive cars and other materials, introducing cyber-crime as a course in secondary school and increase in the arrest and prosecution of cyber-criminals.

CHAPTER FIVE

SUMMARY, DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 INTRODUCTION

This chapter presents the summary, discussion, conclusion and recommendations based on the findings in the study. The research was set out to study the pattern and consequences of cyber-crime in tertiary institutions in Zaria. In order to achieve this, the study was guided by the following objectives; to find out the pattern of cyber-crime, explore the social-attributes of individuals involved in cyber-crime, identify the causes, identify the types of cyber-crime common in Zaria, document the consequences and finally, suggest solution to mitigate against the menace.

5.2 SUMMARY OF MAJOR FINDINGS

The findings from the study showed that a significant number of males who are mostly youths between the ages of 18-30years participated in the research. The study also reveals that majority of the respondents are single. The study also discovered that most of the respondents use the internet and the site assessed by most of the respondents are Google search, social media, academic research, emails, entertainment and news. The study further revealed that cyber-crime is frequent in tertiary institutions in Zaria and mostly perpetrated by youths. It was discovered too that cyber-crime can be committed at anytime of the day but cyber-criminals who are involved in piracy will prefer to commit the act at night because the network will be faster. It was revealed that cyber-café and the home are the major points perpetrating of cyber-crime. In addition, the study shows that cyber-criminals are nicknamed “yahoo yahoo boys” and “yahoo millionaire” who use the following techniques; password cracker, network sniffers, key loggers, honey pot, man in the middle, mathematical model, number extractors, social network, duplication of website, key recorder, password reviler, SQL injection and phone techniques to commit their illegal act. Similarly, cyber-criminals get their proceeds from domiciliary account, money gram and western union.

Findings from the study indicated that hacking, credit card fraud, software piracy, phishing, social network, pin fraud, theft of identity, trafficking of password and credit card number and stealing of direct TV signal are the most common types of cyber-crime that are been perpetrated in Zaria.

As to the socio-demographic attributes of cyber-criminals, the study showed that most cyber-criminals are between the ages of 18-30yrs, who are mostly male and highly knowledgeable in computer. Similarly, it was discovered that those who indulged in cyber-crime could be from any religion and in addition, it was observed that youths from any tertiary institutions in Nigeria and graduates are mostly the perpetrators of this criminal activity. This implies that most of these cyber criminals are educated. From the study, the life styles of cyber-criminals were also identified and it was revealed that cyber-criminals are always on the internet, ride the best automobiles, clubbers and spend money lavishly. Similarly, some of these cyber-criminals indulge the assistance of herbalist/spiritualist to charm their victim.

From the study, it was discovered too that cyber-criminals are motivated by the following factors: excitement to succeed, intellectual pursuit, financial gain, recognition, low rate of conviction, frustration, revenge, display of wealth by corrupt politicians and sabotage. Furthermore, the study found that unemployment, corruption, poverty, peer group influence, easy accessibility to the internet, weak laws and defective socialization are the causes of cyber-crime in the study area.

Results from the study showed that cyber-crime has negative consequences on the society which range from tarnishing the country's reputation internationally to lack of trust and confidence, denial of innocent Nigerians certain opportunity abroad, loss of employment, loss of life and finally, it drives away investors. However, it was further revealed that despite the negative consequences of cyber-crime, it provides a means of survival for cyber-criminals through the sales of pirated software and proceeds they get from other types of cyber-crime.

On the solution to cyber-crime, it was discovered that the crime cannot be totally eradicated but it is possible to check if the following solutions can be followed; youth are empowered by creating jobs; enlighten young ones about the consequences of such act under the law; government regular engagement with IT industries to develop strategies to curtail cyber-crime; zero tolerance to corruption, arrest and immediate prosecution; everybody in the society should be able to report to the law enforcement agencies anyone suspected to be cyber-criminal; our ethical standards are redefined from wealth at all cost to other cherished values; and finally, introducing the topic in the curriculum of secondary school students.

5.3 DISCUSSION OF KEY FINDINGS

This section discusses the key findings from the objectives of the study in relation to other scholar's findings. As to the pattern and consequences of cyber-crime in tertiary institution in Zaria, the study revealed that youths in tertiary institutions and graduates seeking for employment are mostly the perpetrators of this criminal activity. This result is found to have

similarity with past studies. For instance, the report of EFCC (2012), on cyber-criminals caught and penalized shows a large number of the involvement of students and graduates as the main perpetrator of the crime. For example, a 25-year-old student of the University of Ilorin, Imonina Kingsley, was sentenced on four-count of impersonation, possession of fraudulent documents and attempt to obtain money by false pretences and was sentenced 20 years jail term. He was said to have used the false identity of one Mr. Thomas Duke, with the email address given as thomasduke4luv@yahoo.com to send fraudulent mails with intent to defraud unsuspecting victim. Also, Abayomi Lawal Adekunle Nurudeen, a final-year student of Survey and Geo-Informatics Engineering at the University of Lagos, sentenced to 19 years jail term for obtaining \$47,900 from Pee Loo Rosalind Summer, an Australian lady. Similarly, Ferdinand Iheasirim, a 1993 graduate of Accountancy of Abia State University had claimed to Rev Robert McArdle, an Australian and that he was Ben Agwu, a security adviser to Nigeria's president. He was sentenced to 10 years imprisonment. All this are report of EFCC (2012).

The research has shown that hacking, software piracy, credit card fraud, phishing, pin fraud and the use of social network are the commonest types of cyber-crime being perpetrated in tertiary institutions in Zaria. This statement corroborate with past studies on the types of cyber-crime common in Nigeria. For instance, Olugbodi (2010), states that the most prevalent forms of cyber-crime in Nigeria are Website Cloning (phishing), Financial Fraud, Identity Theft, Credit Card fraud, Cyber-theft, Cyber-harassment, Fraudulent Electronic Mails, software piracy and Virus / Worms / Trojans. In addition, Ribadu (2007), stated that the prominent forms of cyber-crime in Nigeria are cloning of websites, falsers representations, internet purchase and other e-commerce kinds of fraud.

Findings from the study showed that youths who are involved in cyber-crime are within the ages of 18-30years who are motivated by the quest for quick luxurious comfort, greed, reputation, vengeance and low chances of being caught. The result of the finding agrees with past studies on the ages of cyber-criminals and motivating factor. For instance, a study by Zero Tolerance (2006), indicates that cyber-criminals are usually within the age category of 18 and 30 years and they indulge in the crime in order to survive and have a taste of good life.

The study further identified the sexes that are involved in cyber-crime. The study showed that males are mostly involved in cyber-crime. This finding can be corroborated with that of Olaide and Adewole (2004) which states that cyber-crimes are male dominated, however, and that female are tender-hearted, feared being caught in evil act, humble, submissive, gentle, emotional and quiet while men are strong and daring.

As to the causes of cyber-crime in Zaria, the findings showed that unemployment, corruption, poverty, peer group influence, easy accessibility to the internet and weak laws are the causes of cyber-crime in the study area. Other studies also agreed with the findings, For instance Okoro (2010), identified the following as the causes of cyber-crime in Nigeria; unemployment, negative role models, lack of adequate policing facilities and knowledge of cyber crime and social gratification. Similarly, Awe (2009), stated that widespread of corruption, harsh economic climate, high unemployment, disregard for the rule of law and lack of transparency and accountability in governance are the main causes of cyber-crime in Nigeria.

Regarding the negative consequences cyber-crime has on the society, it was discovered that such include loss of life, tarnishing the country's reputation internationally, loss of revenue and employment, denial of innocent Nigerians certain opportunity abroad. Similarly, past studies also agreed with this findings for example, Ringwelski (2008), listed the consequences cyber-crime has on the economy to include loss of revenue, wasted time, damaged reputation and reduce productivity.

The study adopted differential association theory which provided the relevant perspective in the study through its nine assumptions. It helped to explain why an individual becomes a cyber-criminal. The theoretical deduction showed that an individual becomes a cyber-criminal if the following three conditions are met: if the individual had learned the requisite skills and techniques for committing the crime, if the individual had learned excess of definitions favourable to crime over definition unfavourable to crime and finally, if the individual had the objective opportunity to carry out the crime. In addition to the theory used, other push factors such as economic, sociopolitical and cognitive factors were identified which could lead an individual to be involved in cyber-crime.

Findings from the studies had shown that those individuals involved in cyber-crime associate with other cyber-criminals either through chat channels (communication) or physically (interaction) in order to perfect their skills and to keep abreast of new techniques and potential targets. The study also revealed, that through these means, the individual develop a rationalization for cyber-crime. This fact tallies with assumption 1 - 4 of differential association theory. That state; Criminal behavior is learned, Criminal behavior is learned in interaction with other persons in a process of

communication, The principal part of the learning of criminal behavior occurs within intimate personal groups, and When criminal behavior is learned. In addition, cyber-criminals have come to realized that corruption thrives in the society and it is uncheck by law enforcement agencies and the law enforcement agencies have not also done much to arrest and prosecute these cyber-criminal due to lack of legislature on cyber-crime, this gives them the opportunity to operate freely without fear of being arrested. This fact also tallies with fifth and sixth assumption of differential association theory, States that an individual will be pushed into deviant behavior depending on their view of the legal code as being favorable or unfavorable. A person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of the law. According to the seventh factor of Differential Association, the finding revealed that the more time an individual spend with cyber-criminals, the more the increase in the frequency that they engage in deviant behavior.

5.4 CONCLUSION

The remarkable development in human history through computer technology has no doubt brought about transformation in all aspects of life, especially in communication and information technology. Nevertheless, the embracement of the internet has come with a lot of mixed feelings despite its numerous advantages to the people. Cyber-crime is the use of computer/internet as an instrument to further illegal ends such as committing hacking, credit card fraud, phishing, pornography, software piracy and theft of intellectual property, stealing identities, unauthorized access, cloning of website amongst others.

It can be inferred from the findings that in Nigeria, people are valued in terms of what they possess and command economically. Conversely, those without economic success are undervalued and the pressure to achieve success is intensified despite the harsh economic condition such as unemployment amongst others. This necessitated the ability of individuals to devise survival strategies and attain economic success by indulging in cyber-crime. However, the increasing rates of cybercrime in the society has become a strong threat to Nigeria's e-commerce growth and has led to ill-reputation internationally and consequently denied some innocent Nigerians certain opportunities abroad. The perpetrators of cyber-crime are not far-fetched; they are our brothers, friends, colleague, distant relatives and neighbours who can be tamed under appropriate circumstances with the right and positive communication, orientation, education and empowerment.

5.5 RECOMMENDATIONS

The recommendations for this research are proffered based on the major findings on the study.

The recommendations are as follows:

1. Youths should be empowered through the creation of jobs.
2. The study has indentified youths within the ages of 18-30years to be the most frequent perpetrators of cyber-crime and in addition, the study has also discovered that these youths are either misguided or misdirected by peers, celebration of unknown wealth amongst others. The study therefore recommends that the young ones should be enlightenment on the consequences of cyber-crime.

3. Government should continue to cooperate with IT industries to develop adequate strategy to fight cyber-crime.
4. There should be zero tolerance to corruption at all levels.
5. Cyber-criminals arrested should be prosecuted immediately to deter a would-be-offender.
6. The findings showed that cyber-criminals live in the society, as such; prevention of cyber-crime requires the co-operation of all the citizens and not just the law enforcement agencies. It is therefore, recommended that everyone should watch and report to law enforcement agencies anyone who indulges in cyber-crime.
7. Our ethical values should be redefined. Vague!!!
8. Finally, the study shows that youths involved in cyber-crime are either in tertiary institutions or have graduated from tertiary institutions; the study therefore, recommends that curriculum which will include courses on cyber-crime, cyber-management and its prevention should be introduced at both tertiary and secondary schools to take care of the present social changes.

REFERENCES

Abdulhamid, S.M, Haruna, C. and Abubakar, A. (2011) Cybercrimes and the Nigeria Academic Institution Networks. *The IUP Journal of Information Technology*. Vol VII No 1. pp11.

- Ahmed, A.A. (2010). *Hack No More, Internet Security: Attacks and Defence*. Ahmadu Bello University Press Limited, Zaria Nigeria, pp 71.
- Aghatise, E.J. (2006). *Cyber-crime Definition*, Computer Crime Research Centre. Retrieved September 20, 2011 from www.crime-research.org
- Akande, F.F. (2007). *Issue in Humanities and Technology*, Integrity Publication, Ilorin.
- Akpabio, I.I. and Ebong, F.S. (2009). *Research Methodology and Statistics in Health and Behavioural Sciences*, UNICAL Printing Press, Calabar, Nigeria. pp 91.
- Ajewole, A. (2010). Curbing Cyber crime in Nigeria. Fighting the Masked Enemy and Promoting Productive Alternative for the Youth. Retrieved October 8, 2011 from <http://www.primopdf.com>.
- Arase, S. and Obaedo, A. (2009), *Policing Nigeria in the 21st Century*, Spectrum Book, Ibadan, Nigeria. pp 298 – 302.
- Awe, J. (2009). *Fighting Cybercrime in Nigeria*. Retrieved September 10, 2011 from <http://www.jidaw.com/itsolutions/security3.html>.
- Ayantokun, O. (2006). *Fighting Cyber-Crime in Nigeria, Information-System*, Retrieved September 10, 2011 from www.tribune.com.
- Broadhurst, R.G. and Grabosky, P.N. (2005). *Cyber-Crime: The Challenge in Asia*, Hong Kong University Press, Hong Kong. Pp 15- 81.
- Dambazau, A.B, Jumare, M.M. and Yakubu, A.M. (1996). *Issues in Crime Prevention and Control in Nigeria*, Baraka Press and Publishers Ltd Kaduna, Nigeria.
- Ehimen, O.R. and Bola, A. (2010). Cybercrime in Nigeria, *Business Intelligence Journal*, Vol. 3 No.1 pp. 98.
- Erinosho, L, Obasi, I.N. and Maduekwe, A. (2002). *Interdisciplinary Methodologies in the Social Sciences*, Auscon Fireseed and Co Ltd, Abuja, Nigeria.
- Fischer, J.R, Halibozek, E. and Green, G (2008). *Introduction to Security*, Linacre House, Jordan Hill, Oxford. pp 299-441.
- Federal College of Education Zaria Students College Handbook (Revised 1999).
- Gyong, J.E (2011). Basic Component of a Research Project in Sociology, *A Paper Presentation at the In-House Training, Department of Sociology, ABU, Zaria*.
- Haralanbos, M, Holborn, M. and Heald, R. (2008). *Sociology: Theme and Perspectives*, Harper Collins Publishers, London, UK.

- Hidayatullah, K (2000), *Cyber Crime And Its Consequences*, National Law University Raipur (Chhattisgarh) village Upperwara, Tehsil Abhanpur, New Raipur (C.G)
- History of Ahmadu Bello University Retrieved from www.abu.edu.ng/about/history.php-cached
- History of Kaduna State, Retrieved Apr 8, 2012 from http://en.wikipedia.org/wiki/kaduna_state
- History of Nuhu Bamalli Polytechnic Retrieved from www.nuba.ng.org
- History of Zaria retrieved Apr 8, 2012 from [http://en.wikipedia.org/wiki/zaria_\(disambiguation\)](http://en.wikipedia.org/wiki/zaria_(disambiguation))
- Theory in sociology Retrieved September 14, 2011 from <http://www.criminology.fsu.edu/crimtheory/sutherland.html>
- Imhof, R. (2010). *Cybercrime and Telecommunication Law*, Rochester Institute of Technology USA.
- Information and Communication Technology Spending (2005). From Wikipedia, the free Encyclopedia.
- Internet Crime Complaint Center, (2010). Internet crime report Retrieved from http://www.ic3.report.nw3c.org/docs/2010_ic3_report_02_10_11_low_res_pdf.2011
- Kumar, K. (2003). *Cyber Laws, International Property and E-commerce Security*, Dominant Publishers and Distributors, New Delhi.
- Longe O.S. and Chiemeka S.C. (2008). Cyber Crime and Criminality in Nigeria. What Roles are Internet Access Points in Playing? *European Journal Social Sciences* Vol 6, No 4, pp 132-139.
- Matsueda, R.L (2000). *Differential Association Theory*. Seattle, WA, University of Washington.
- McConnell, (2000). Cybercrime and Punishment, *Archaic Laws Threaten Global Information*, www.mcconnellinformation.com.mcconnellinternational L.L.C
- McQuade, S. (2009). *The Encyclopedia of Cybercrime*, Green Wood Press, Westpoint Connecticut, London.
- Morley, D. and Parker, C.S. (2007). *Understanding Computers, Today and Tomorrow* 11th Edition, Published by Thomson Course Technology, USA. pp 312

- National Population Commission (2006), 2006 Population and Housing Census of the Federal Republic of Nigeria, national population Commission.
- Ogbunwezeh, E.F. (2006). *EFCC and Cybercrime The True Lesson*, Retrieved from www.nigeriavillagesquare.com
- Olaide, M. and Adewole, R. (2004). *Cyber Crime Embarrassing for Victims*. Retrieved September 2011 from <http://www.heraldsun.com.au>
- Olayiwola, A.O. (2007). *Procedures in Educational Research*, Hanijam Publications, Ahmadu Bello Way, Kaduna, Nigeria. pp 106.
- Olugbodi, K. (2010). *Fighting Cyber Crime in Nigeria*, Retrieved September 10, 2011 from http://www.guide2nigeria.com/news_articles_about_Nigeria.
- Osuala, E.C. (1992). *Introduction to Methodology*, African Fep Publishers Limited, Nigeria.
- Oyesanya, F. (2004). *Nigerian Internet 419 On The Loose*. Retrieved October 8, 2011 from <http://www.nigeriavillagesquare.com>.
- Oyewole, A.S. and Obeta, A. (2002). *An Introduction to Cyber Crime*. Retrieved September 2011 from <http://www.crime-research.org/articules/cyber-crime>.
- Pati, P. (2003), *Cybercrime*. Retrieved from www.nivi.org
- Planetindia, (2001). *Introduction to Cyber Crime*. Retrieved October 9, 2011 <http://cybercrime.planetindia.net/intro.htm>.
- Ribadu, N. (2007). *Cybercrime and Commercial Fraud: A Nigerian Perspective, A paper presentation at the Modern Law for Global Commerce, Vienna 9-12 July 2007*.
- Ringwelski, M. (2008). *Effects of Cyber Crime*. Retrieved from http://www.ehow.com/about_5052659_effects-cyber-crime.html#ixzz1gaX6daue.
- Roger, E. (1995). *Diffusion of Innovation*, Retrieved September 12, 2011 from http://enwikibooks.org/wiki/communication_Theory/Diffusion_of_Innovations.
- Rogers M.K. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behaviour. An Exploratory Study*, University of Manitoba, Winnipeg, Manitoba.
- Salihu, T. (2006). *Impact of Computer Appreciation in Military Technology, A Commandant's Paper submitted to Nigerian Army School of Military Police, Zaria*.
- School of Postgraduate Studies ABU (2010), *Regulations Governing Higher Degree Studies*, Zaria, Nigeria: ABU Press Limited.

- Schell, B.H. and Martin, C. (2004). *Cybercrime: A Reference Handbook*, ABC-CLIO Inc, Santa Barbara, California. pp 4.
- Sesan, G. (2010). *The New Security War*, Retrieved from http://www.pcworld.com/article/122492/the_new_security_war.htm#tk.mod-rel.
- Shinder, D.L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*, 800 Hingham Street, USA, Syngress Publishing Inc.
- Tade, O. and aliyu, I. (2011), Social Organization of Internet fraud among University Undergraduates in Nigeria. *Internation Journal of cyber Criminology*. Vol 5(2). pp 860-875
- Thomas, D. (2011). *Cybercrime in Nigeria*, Retrieved September, 2011 from <http://www.idgnews.net/>
- Umar-Ajijola, J. (2010). *Microsoft Combats Cybercrime in Nigeria*, Retrieved from <http://www.pcworld.com/businesscenter/article/205051/cybercrime>.
- Umar-Ajijola, J. (2010). *Fighting Cybercrime in Nigeria*. Retrieved from http://blogs.technet.com/b/microsoft_on_theissues_africa/archive/2010/12/9/fighting-cybercrime-in-nigeria.aspx.
- Vladimir, G. (2005). *International Cooperation in Fighting Cyber Crime*. Retrieved from www.crimeresearch.org.
- Wall, D.S (2001), *Crime and The Internet*, London Routledge Publisher.
- Wall, D.S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, 65 Bridge Street, Cambridge, Uk.
- Yar, M. (2006). *Cybercrime and Society*, London, Sage Publication Ltd.
- Young Media Association (2007). *The Internet: Benefits, Danger and strategies*. Australia Young Association.
- Zero Tolerance (2006), 'The Portrait of a Yahoo Yahoo Boy' *Economic and Financial Crime Commission*, Vol 1 No 3 pp 38-39.

APPENDIX I

QUESTIONNAIRE

Dear respondent,

I am a post graduate student of the Department of Sociology, A.B.U Zaria carrying out a research on the pattern and consequences of cyber-crime in tertiary institution in Zaria. This is in partial fulfillment of an award of M.Sc Sociology. All information provided will be strictly confidential for academic purposes only. Thank you sir

Instruction: Please tick or respond where appropriate

SECTION A: SOCIO-DEMOGRAPHIC DATA OF RESPONDENT

1. Sex: (a) Male () (b) Female ()
2. Age: (a) Below 18 () (b) 20-24 () (c) 25-30 () (d) 31-35() (e) 36-above ()
3. Religion (a) Islam () (b) Christianity () (c) Traditional Religion ()
4. Marital Status: (a) Single () (b) Married () (c) Divorce () (d)Widow ()

SECTION B: PATTERN OF CYBER-CRIME

5. Do you access/use the internet?(a) Yes () (b) No ()
6. Which activity do you spend most time doing on the internet? Please tick as many as apply.

Serial	Site visited	Response
a.	Google search	
b.	Sport	
c.	Email	
d.	Internet phoning	
e.	Social media (facebook and yahoo messenger)	
f.	Academic research	
g.	Pornography	
h.	Games	
i.	Media, entertainment and news	
j.	Spamming	
k.	Piracy	

7. Have you heard of the term Cyber-Crime? (a) Yes () (b) No ()
8. How frequent do you hear reports on cyber-crime?(a) Frequent () (b) Not frequent() (c) Undecided ()
9. Who are those involved in perpetration of cyber-crime? (a) Youths () (b)Adult () (c) Aged ()
10. At what time of the day is cyber-crime usually been perpetrated? (a) Day () (b) Night () (c) Any time of the day ()
11. Where is cyber-crime perpetrated point? Please tick as many as apply.

Serial	Cyber-crime perpetrated point	Response
a.	Cyber-café	
b.	At home	
c.	Government offices	
d.	Private organization network	

12. Please tick as many as apply the nomenclatures listed below given to those who engage in cyber-crime.

Serial	Nomenclatures of cyber-criminal	Response
a.	Yahoo Yahoo Boyz	
b.	Yahoo Millionaire	
c.	Yahoo Zee	
d.	Forex trade	

13. Please indicate which of these type of techniques/tools listed below are used by cyber-criminals to perpetrate their act? (please tick as many as apply)

Serial	Types of techniques	Response
a.	Exploit	
b.	Port scanner	
c.	Vulnerability scanner	
d.	Password cracker	
e.	Network sniffer	

f.	Key loggers	
----	-------------	--

14. Apart from the aforementioned, please list other techniques/tools used by cyber-criminal to perpetrate their criminal act?.....

SECTION C: TYPES OF CYBER-CRIME

15. Which of the following type(s) of cyber crime do you know are common in Zaria? (Please tick as many as apply)

Serial	Types of cyber-crime	Response
a.	Cyber/identity theft	
b.	Cyber-stalking	
c.	Malicious program/Virus dissemination	
d.	Pornography	
e.	Credit card fraud	
f.	Hacking	
g.	Sweet heart swindle (Social network)	
h.	Cloning of website/Phishing	
i.	Software piracy	
j.	Cyber defamation	

16. Aside the above mentioned types of cyber-crime, list other type(s) common within Zaria?.....

SECTION D: SOCIAL ATTRIBUTES OF CYBER-CRIMINALS

17. Have you seen a cyber-criminal before? (a) Yes () (b) No ()
18. Do you have friends who engage in cyber-crime? (a) Yes () (b) No ()
19. Please indicate your opinion/response to the following on the features of the individuals involved in cyber-crime?
- (i) Age (a) 18 - 30 () (b) 31 - 40 () (c) 41 and Above () (d) Undecided ()
- (ii) Sex (a) Male () (b) Female () (c) Both Male and Female ()

- (iii) Religion (a) Islam () (b) Christianity () (c) Traditional Religion ()
(d) Any Religion ()
- (iv) Individual qualification (a) Primary Education () (b) NCE () (c) Polytechnic () (d) University () (e) Others, please specify.....
- (v) Marital status of parents (a) Married () (b) Divorce () (c)Widow () (d) Undecided ()

20. Please tick as many as apply on the life style of cyber-criminals in line with the following?

Serial	Life style of a cyber-criminal	Response
a.	Riding the best automobiles	
b.	Mainly clubbers	
c.	Hang out in upscale pubs	
d.	Spend money lavishly	
e.	Date the most beautiful ladies	
f.	Live like kings in the society	
g.	Indulged in ritual activities	
h.	Always on the internet	

SECTION E: CAUSES OF CYBER CRIME

21. List the motivating factors that encourage individual’s involvement in cyber-crime?

.....
.....

22. Please indicate your responses (strongly agree (SA), agree (A), undecided (UD), strongly disagree (SD), disagree (D) to the statement on the causes of cyber-crime in Zaria?

Serial	Causes of cyber-crime	Rating				
		SA	A	UD	SD	D
a.	Poverty					
b.	Unemployment					

c.	Peer group influence					
d.	Defective socialization					
e.	Weak laws/absent of existing law on cyber-crime					
f.	Corruption					
g.	Easy accessibility to the internet					

SECTION F: CONSEQUENCES OF CYBER-CRIME

23. Do you think cyber-crime has any negative consequence(s) on the economy? (a) Yes () (b) No ()
24. What are the negative consequences associated with cyber-crime? Please tick as many as apply.

Serial	Consequences of cyber-crime to the society	Response
a.	Loss of life	
b.	Tarnishing the country's reputation internationally	
c.	Denial of innocent Nigerians certain opportunity abroad	
d.	Loss of revenue	
e.	Loss of employment	
f.	It is inimical to progress and development of the country	
g.	Lack of trust and confidence which is currently hindering profitable transaction.	

SECTION G: SOLUTIONS TO CURB CYBER-CRIME

25. Do you think that cyber-crime can be controlled? (a) Yes () (b) No ()
26. If yes, tick as many as apply to the following statements on the solution to tackle the menace

Serial	Solution to the menace	Response
a.	Zero tolerance to corruption.	
b.	Empowerment of youths.	

c.	Redefine our ethical standards.	
d.	Arrest and immediate prosecution of cyber-criminals	
e.	Introduce cyber-crime as a course in the curriculum of secondary school Students.	
f.	Enlighten young ones about the consequences of such actions under law.	
g.	Report to the police or other concerned authorities anyone we might suspect of engaging in cybercrime.	
h.	Government regular engagement with IT industry to develop strategies that can prevent and curtail cyber-crime.	

27. Aside the aforementioned solutions to tackle the menace, please suggest other solutions you think can be done to mitigate the rising rate of cyber-crime in the society or make the internet be of positive use only?.....

APPENDIX II

INTERVIEW GUIDE FOR CYBER-CAFÉ OPERATOR

The researcher is a student from ABU Zaria carrying a study on pattern and consequences of cyber-crime in tertiary institutions in Zaria. The study is required for academic purpose and you are reassured of strict anonymity and confidentially about information given. The interview will take about 45 minutes or thereabout and I will want to use a tape recorder so that I can get all the information better. Do I have your permission to continue, thank you sir?

1. General characteristics of the informant
 - a. Age
 - b. Sex
 - c. Educational level

2. Pattern of cyber-crime in tertiary institutions in Zaria.

Probe for:

- a. How long have your cyber-café been in existence.

- b. Hours of operation per day?
- c. Frequent customers?
- d. Definition of cyber-crime.
- e. Have cyber-crime ever been committed in your cyber-café, frequency, time, the number of people caught, the year and what was done to them.
- f. Persons usually involved in cyber-crime and time of perpetration.
- f. Techniques cyber-criminals use.
- g. Have there been changes in the techniques.
- h. Does the techniques cyber-criminals adopt yield results?
- i. How do cyber-criminals get their targets (victims)?

Types of cyber-crime common in the study area

3. What are the various types of cyber-crime perpetrated by individuals?

Probe for:

- a. General types of cyber-crime.
- b. The types of cyber-crime in vogue in Zaria.
- c. Whether there have been changes in recent times.

Social attributes of cyber-criminals

4. What can you say about the perpetrators of cyber-crime in terms of the following attributes?

Probe for:

- a. Age bracket.
- b. Sex.

- c. Religion.
- d. Education background.
- e. Family background.
- f. Life style

Causes of cyber-crime

5. What do you think could be the factors responsible for the involvement of youths in cyber-crime?

Probe for:

- a. Motivating factors
- b. Causal factors; (socio-economic, family background, societal factor amongst others)

Consequences of cyber-crime

6. What do you think are the consequences of cyber-crime on the economy, individual and parents?

Probe for:

- a. Negative consequences
- b. Positive consequences.

Solutions

7. What do you think can be done to make the internet be of positive use only?

Probe for:

- a. measure to be taken by individual.
- b. Measures to be taken by parents.

- c. Measures to be taken by the government

Thank you very much for your time. Your contribution have been helpful

APPENDIX III

INTERVIEW GUIDE FOR LECTURERS OF COMPUTER DEPARTMENTS IN TERTIARY INSTITUTION

The researcher is a student from ABU Zaria carrying a study on the pattern and consequences of cyber-crime in tertiary institutions in Zaria. The study is required for academic purpose and you are reassured of strict anonymity and confidentiality about information given. The interview will take about 45 minutes or thereabout and I will want to use a tape recorder so that I can get all the information better. Do I have your permission to continue, thank you sir?

1. General characteristics of the respondents:

- a. Age
- b. Sex
- c. Educational level

2. Pattern of cyber-crime in tertiary institutions.

Probe for:

- a. Definition of the crime.
- b. Person usually involved in cyber-crime.
- c. Mode of operation.
- d. Perpetration point of the crime.
- e. Techniques cyber-criminals use.
- f. Does the techniques adopted yield results.
- g. How do cyber-criminals get their targets (victims).

Types of cyber-crime

3. What are the type(s) of cyber-crime common in Zaria.

Social attributes of cyber-criminals

4. Have you seen a cyber-criminal and do you have friends who engage in the crime.

5. From your experience and nature of your profession, what are the features of those involved in cyber-crime?

Probe for:

- a. Age range.
- b. Sex.
- c. Religion.
- d. Marital Status.
- e. Family size and position of the student within his/her family.
- f. Employment status of the parents.
- g. Specific occupation of parents.
- h. Family history (are the parent separated).
- i. Socio-economic background of the family.

Causes of cyber-crime

6. From the point of view of your profession and knowledge, what are the factors responsible for the involvement of youths in cyber-crime?

Probe for:

- a. motivating factors
- b. Causal factors (socio-economic status of the parents, defective socialization, moral decadence, accessibility to the state of the art technology).

Consequences of cyber-crime

7. What danger does cyber-crime pose to the society?

Solutions

8. What do you think can be done to eradicate or reduce to the barest minimum cyber-crime in the society?

Thank you very much for your time. Your contribution have been helpful

APPENDIX IV

INTERVIEW GUIDE FOR THOSE WHO INDULGE IN CYBER-CRIME

The researcher is a student from ABU Zaria carrying a study on the pattern and consequences of cyber-crime in tertiary institutions in Zaria. The study is required for academic purpose and you are reassured of strict anonymity and confidentiality about information given. The interview will take about 45 minutes or thereabout and I will want to use a tape recorder

so that I can get all the information better. Do I have your permission to continue, thank you sir?

1. socio-demographic information

- a. Age
- b. Sex
- c. Religion
- d. Educational level
- e. The marital status of parents
- f. Employment status

2. Pattern of cyber-crime

Probe for:

- a. How long have you been doing this activity?
- b. Where do you access the internet?
- c. What do you use to access the internet?
- d. What time of the day do those who engage in this activity perpetrate their criminal act?
- e. What are the various techniques used in this activity?
- f. What type of technique do you use to get your victims?

3. What are the type(s) of cyber-crime you indulge in?

Probe for:

- a. Types of cyber-crime
- b. Why that particular type of cyber-crime.

4. What are the features of those who do what you do?

Probe for:

- a. Sex
- b. Age
- c. Religion
- d. Family size
- e. Marital status (amongst other)
- f. Education background

5. Why do you engage in this kind of activity?

Probe for:

- a. motivating factors
- b. Causal factors

6. Consequences of cyber-crime

Probe for:

- a. Do you think cyber-crime has negative consequences? If yes, name them.
- b. Does cyber-crime have any economic benefit for you, if yes name them.

7. What do you think can be done to make the internet be of positive use only?

Thank you very much for your time. Your contribution have been helpful