IMPLICATION OF CYBERCRIME AMONGST STUDENT IN THE UNIVERSITY OF BENIN (UNIBEN), BENIN CITY, EDO STATE, NIGERIA.

BY

Esther Ceremi OKEY
SSC1809949

DEPARTMENT OF SOCIOLOGY AND ANTHROPOLOGY
FACULTY OF SOCIAL SCIENCES
UNIVERSITY OF BENIN
BENIN CITY

SEPTEMBER, 2023

IMPLICATION OF CYBERCRIME AMONGST STUDENT IN THE UNIVERSITY OF BENIN (UNIBEN), BENIN CITY, EDO STATE, NIGERIA.

BY

Esther Ceremi OKEY
SSC1809949

A PROJECT SUBMITTED TO THE DEPARTMENT OF SOCIOLOGY AND ANTHROPOLOGY, FACULTY OF SOCIAL SCIENCES, UNIVERSITY OF BENIN, BENIN CITY, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF SCIENCE (B.SC.) DEGREE IN SOCIOLOGY AND ANTHROPOLOGY

SEPTEMBER, 2023

CERTIFICATION

This is to certify that this project work was carried out by **Esther Ceremi OKEY** with Matriculation Number**: SSC1809949** of the Department of Sociology and Anthropology, Faculty of Social Sciences, University of Benin, Benin City, Edo State, Nigeria.

_____	_____
Dr. Michael Ndisika	**Prof. A.O Dokpesi**
(Project Supervisor)	***(Head of Department)***
Date: _____	**Date:_____**

DEDICATION

This project is dedicated to God Almighty whom through his infinite mercies saw me through and made it possible to accomplish this programme.

.

ACKNOWLEDGEMENTS

I wish to express my profound gratitude to God Almighty. To all those who contributed directly and indirectly making this work a huge success.

Special appreciation to my project supervisor. Dr. Michael Ndisika, My course adviser Dr. Jude Akaba, my HOD, Professor Augustine Dokpesi and all lecturers in the department of sociology and anthropology for their immense love and guidance in through course of this research and my stay in the University of Benin.

Particularly, I am indebted to my parents; Pastor and Mrs. Okey Yesuf and my ever loving siblings. Shoutout to Daniel Okey; Okey first son who have been supportive through and through. Also to Mr. and Mrs. Odum who have been a strong pillar in my life. Also to immediate elder sister as well as my close friends Okey Faith, Precious, Blessing Ikenna, Emma, Blessed. Baby gal love you all.

Furthermore I want to specially appreciate Ndine Lawrence a senior colleague from the Department of Sociology and anthropology. Lastly, special acknowledgment goes to the SAA class of 2022, (social scholars). To my family VFCF (Uniben/UBTH chapter), I love you all. To everyone I failed to mention thank you all for your support love prayers and care, God bless you.

TABLE OF CONTENTS

ABSTRACT

The study sought access the implications of cybercrime amongst students in the University of Benin. It is an empirical survey of the students of the University of Benin. Survey research design was adopted for the study. The study was conducted University of Benin, Benin City, Edo State, Nigeria. The population of the study comprised of students from the tertiary institution. Nassiuma formula was used to cumulate the sample size from the entire population and this gave a total of 100 respondents that constituted the sample size for the study. The Main Instrument used in this study was a questionnaire titled "Implications of cybercrime amongst students in University of Benin". The researcher subjected the data generated for this study to appropriate statistical techniques such as percentage analysis for answering the research question. The study revealed that there is significant influence of the implications of students' involvement in cybercrime. Hence, the study concluded that certain precautionary measures should be taken by students while using the internet which will assist in challenging this major threat Cybercrime. One of the recommendations was that federal and state government, as well as educational communities should intensify campaigns on cybercrime awareness among Nigerian undergraduate students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act with attendant adverse consequence of jeopardizing their educational accomplishment when conviction.

SECTION ONE

INTRODUCTION

1.1 Background of the Study

The initial intent of advancing the internet was not to propagate crime but wiring the world together through information technology (Augustine, 2016). However, the cyberspace has created new opportunities for global attacks on the infrastructure of countries. The internet has become a necessary evil with two sides to it; the positive and the negative (Magele 2011). Cybercrime also referred to as cyberfraud has grown prominence as the computer has become central to commerce, entertainment, and government (Dennis, 2019). In (Maitanmi, 2013) cybercrime was defined as a type of crime committed by criminal who make use of a computer as a tool and the internet as a connection in order to reach a wide range of objectives such as illegal downloading of data and files, piracy, spam mailing etc. Okonigini (2002) asserts that cybercrime is any activity that entails individual encroaching illegally into any information technology infrastructure through the use of computer or computer related devices. In modern societies, crimes and the ways they are planned and executed have changed with the levels of technological advancement and sophistication, especially following the advent of ICT in general and social media in particular (Angioha, Enukoha, Agba, & Ikhizamah, 2020; Ukwayi,

Akintola, & Angioha, 2019; Ukwayi, Obafaye & Akintola 2019) to take off in the early 2,000's when social media came to life. Today, the world is more digitally connected than ever before. Criminals take advantage of this online transformation to attack online systems, networks and infrastructure (www.interpol.int).

The concept of cybercrime is historical as it was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960's (Maitanmi 2013). According to (Lakshimi, 2015) as at 2003, the United States and South Korea have the highest cyber-attacks of 35.4% and 12. 8 respectively. Global cybercrime damage costs as at 2021 was expected to breach US $6 trillion an annum. That is almost one-fourth of the US GDP or twice the GDP of India. Cyber attackers are disrupting critical supply chains, at least 4 times more than in 2019 (www.theirmindia.org, 2021). The threat of from cybercrime is multidimensional cutting across borders government, economies, nations across the globe. The DBIR report shows that North America is most threatened in the world facing a barrage of cyber-attacks from diverse sources and method. A 2023 data breach report from Verizon found that almost 70% of all recorded data breaches happen in the North America i.e USA and Canada. Cybercrime is a growing is a growing issue for European countries. It comprises of 7% of the world population but almost a fifth of

its internet users and every one of these 320 million citizen usually fall victim to criminal activity from everywhere on the planet since internet eliminate distances bringing the general public and cyber-crime to close proximity. Although, it is difficult to estimate the precise financial cost of cybercrime (Anderson et al., 2013; Anderson et al., 2019), statistical evidence from governments and industries indicates that the economic losses caused by cybercrime are extremely enormous and are still rising rapidly (McAfee, 2021).

Cybercrime is a big issue in Africa. Jones (2011) shows how the African region had been regarded as a backward and developing region which this has featured into her ICT world. A Deloitte survey published by Buddecomm, an independent research and consultancy company in the 8year 2011 found that banks in Kenya, Rwanda, Uganda, Tanzania and Zambia alone had lost $245 million to cyber fraud. In Africa, poverty, unemployment and in development are the major cause for growth of cybercrime in the region. Many watchers are warning that Africa is becoming a major source of cybercrime. It is proven that 39.6% African users of internet are actually Nigerian, hence that could be one of the contributing factors to the increase of internet crime in Nigeria (Hassan 2012).

In Nigeria, cybercrime is prevalent illegal activity. Alemika (2007) note that currently cybercrime has become a norm in the Nigerian society today. Cybercriminals in Nigeria are notorious for luring people across the planet into fraudulent scams via spam mails, cash-laundering e-mails, and Criminals involved in the advance fee fraud schemes (419) known as "yahoo yahoo" an d the perpertuators are popularly referred to as "yahoo boys" in Nigeria. Ngozi (2016) asserted that the level at which Nigerian youths are delving into cybercrime is quite alarming; It seems Nigeria holds a image of fraudulent citizens involved in what is referred to as "419" mails named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud. Nigeria has earned its place as a popular haven for fraudsters and cyber criminals and now ranks third in terms of global internet crimes perpetrated. Going by the nature that cybercrime can tarnish the image from the individual to organisational level, it becomes very expected, to find out the implications and possible remedies. Aghatise (2006), asserted that most perpetrators of cyber frauds in Nigeria are students in polytechnics, universities, and other tertiary institutions. High educational attainment is also likely to be associated with cybercrime, given that cybercrime usually requires some level of computer skills and IT knowledge (Holt and Schell, 2011; Asal et al., 2016). Akpan (2016), reported that cybercrime has put the Nigerian students in a serious quest for money other than the real deal of getting university education.

1.2 Statement of Problem

The very purpose for Education is to equip student with great knowledge which would be profitable service now and in the future. These body of knowledge is both inclusive of academic knowledge and moral awareness. However, in recent years, cyber fraud has emerged as a new type of criminal activity in our higher education institutions, causing economic and educational damage (Ehimen, 2010). Cybercrime in largely perpetuated by student in tertiary institutions and are socially tagged "yahoo yahoo boys" (Tade 2011 and Aliyu 2011). It has been observed that it is a tool that gets in the way of effective learning. These findings are consistent with those of previous studies that have found a slink between cybercrime and student performance, including those by Lin and Chiang (2017), Igba, Igba, Nwambam, et al. (2018), Ajayi (2019), and Adegbola and Fadara (2022). This is a fact problem because the spate of cybercrime activities in higher institutions south-south Nigeria has assumed a worrisome dimension. The emergence of "yahoo boys" is debilitating the national economy (Ogwezzy, 2012); the number of students who spend valuable hours browsing dubious websites at the expense of academic knowledge is telling on the dwindling level of performance in school examinations (Ige, 2008). While the law enforcement agencies have not been able curtail the act amongst student in tertiary institutions, the prevalence and the effects continue to hit hard on Nigeria economy, education, family as

well as other social institutions. On this premise, this research seeks to understand the increasing phenomenon behind cybercrime amongst student using the student in university of Benin as area of study. The study seeks to understand the dilemma of student that prompts to partake in this notorious act. It seeks to understand how people have come to perceive theses act including the perpetuators, victims and beneficiaries. It seeks to understand the governments and individualistic perspective to this menace.

1.3 Research Questions

From the problem stated above it is imperative that the following questions are asked.

The main research Question will be: What are the implications of cybercrime among students in the University of Benin.

The study also seeks to attempt the following Specific research questions

a. what is the rate of involvement in cybercrime amongst the student if University of Benin.
b. what are the form/types of cybercrime practiced by students in the University of Benin.
c. what are the possible causes of cybercrime among student in University of Benin (Uniben)
d. what are there possible solutions to cybercrime amongst students in the University of Benin.

1.4 Objectives of the Study

The main objective of this study is to identify the implications of cybercrime amongst student in the University of Benin. The Specific objectives to this study are:

a. To examine the rate of student involvement in cybercrime in the university of Benin

b. To identify some of the forms/types of cybercrime practices among students in university of Benin.

c. To determine the causes of cyber fraud amongst student in University of Benin (Uniben)

d. To predict possible remedies to the situation.

1.5 Scope of Study

The study focused on the implications or effects of Cyber Crimes among students in the University of Benin. The Researcher focused on the intended and unintended consequences of fraudulent activities of students in the tertiary institution; University of Benin (UNIBEN), Edo State Nigeria.

It is a research that has established the fact that a large proportion of Nigerian cyber criminals are college-based youths and it goes further to explain that Cybercrime is one of the most prevalent types of crime committed by tertiary institution students in Nigeria (Aransola & Asindemade 2011; Tade & Aliyu

2011). The findings in the research is based on the data gathered from various books and online sources and furthermore the opinions of the students in the University of Benin.

1.6 Significance of Study

The findings and recommendations from this study would serve as indispensable instruments in policy formulation and research by students in the future. It will also give the academic world a better understanding of the perception of students about cybercrime

1.7 Definition of Key Terms

Cyber: The use of computer system or internet.

Crime: An illegal act punishable by law.

Cybercrime: The use of computer to commit an illegal act.

Internet: A global computer network providing a variety of information and communication facilities, consisting of interconnected network**.**

Data Breach: Data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, altered or used by an individual unauthorized to do so.

Piracy: The unauthorized use or reproduction of another's work.

Spam Mailing: unsolicited email messages, usually sent in bulk to a large list of recipients.

Yahoo Yahoo: The term is used in Nigeria to refer to cybercriminals (cyber fraudster)**.**

419: The term used to describe fraud in Nigeria.

SECTION TWO

LITERATURE REVIEW

Many literature exit on the subject matter. This chapter is structured into several parts; The concept and History of cybercrime in Nigeria, rate of student involvement in cybercrime the types of cybercrime, causes of cybercrime, implications of cybercrime, remedies to curbing student's involvement in cybercrime, theoretical frameworks and lastly research hypothesis. All these will be explicitly explained backed up with relevant literature.

2.1 The Concept and the History of Cyber Crime in Nigeria

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials (Brush, Rosencrance and Cobb, 2020). Halder and Karuppannan, (2011) define cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice

boards and groups), and mobile phones (SMS/MMS). Thomas and Loader (2000), conceptualised cybercrime as those computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Maat (2004), proposed a definition for cybercrime which encompasses all illegal activities where the computer, computer systems, information network or data is the target of the crime and those known illegal activities or crime that are actively committed through or with the aid of computer, computer systems, information network or data. Since it has become a commonly used term different scholars have referred to it to mean illegal activities related to ICT inventions (Olowa, 2009). For the Internet Crime Complaint Center (ICCC ,2010), cybercrime is any act of illegal perpetuating using any aspect of the internet in terms of browsing, pinging, chatting and/or email. Cyber Crime is broadly defined as any illegal activity that involves a computer, another digital device or a computer network.

In recent times, individuals, organisations, government rely on the internet and other information technology to carry out her daily activities such as education, business, entertainment, banking, security and so on and so forth. While this bring about enormous gain in productivity, it has also created a loophole which retards society. Cybercrime is a new trend that grows gradually as the internet gradually becomes part and parcel of our society.

The continuous increase of this crime is something that should not be overlooked. The effect of this crime can affect individuals to the nation as whole. cybercrime fraud or deception which makes use of the and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance (Warf, 2018). Cybercrime is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. It is, however, differentiated from theft since, in this case, the victim voluntarily and knowingly provides the information, money or property to the perpetrator (Brenner, 2009). It is also distinguished by the way it involves temporally and spatially separated offenders. Internet fraud can occur even if partly based on the use of Internet services and is mostly or completely based on the use of the Internet (Fisher and Lab, 2010). Cybercrime in Nigeria has continued to increase rapidly. According to Bengal, Babatope and Bankable, (2012) cybercrime as at 2002-2003 was 5% and in 2012, 30% and it has been increasing drastically ever since.

Consequently recent years have seen significant upsurge of victims of online fraud within Nigeria (Idom and Tormusa 2016, MBA et al 2017, Ndubueze, 2020) and outside Nigeria (e.g. Leukfeldt et al, 2020), all originating from Nigeria on cybercriminal. Fraudulent practices through cyber-crime has raised up emergency millionaires, even billionaires student

which is venomous to our economic growth as most of such funds acquired, ill-gotten wealth are not been used productively to promote the economy. Conclusively, Nigeria's image has continuously been the worse for it. It has been seriously battered internally and externally.

Literarilly, the use of Yahoo Messengers for fraudulent activities started in the late 90s, hence the use of term "Yahoo" or "Yahoo Yahoo" to refer to cybercrime/fraud in Nigeria. Yahoo boys came in stages, at the initial stage were those who started in the early 2000s using mailers to " bomb" (a term used to describe accessing of websites or platforms to get victims) sites in order to get victims/client demanding a particular sum of money to redeem lottery tickets. Then came the era of the real G-men by 2006\2007 called the Yahooze. This set was specialised and focused in love scamming.

Those from the second era have pumped their ill-gotten wealth into legitimate businesses to cover up their crime. The recent era of Yahoo boys from 2010 till date are usual young people who are on the quest to make it in life fast and easy. They are usually careless and extravagant with their lifestyle. With advancement in technology, scamming platforms are now numerous to choose from in order to get clients. They are however traced by the authorities such as the Economic and Financial Crimes Commission (EFCC). Apart from using websites, the present generation of yahoo boys now use social media platforms for bombing and the most commonly used

is Facebook, which is the reason they hack Facebook accounts or buy them like a commodity. Another form of it is Facebook dating, which is often with women from different countries to exhort them of some money. It is an enhancement to their predecessors “love scamming” method.

Soaked in greed and desperation to have wealth by all means, they now aid their activities with black magic and charms and this particular one is called Yahoo Plus. Some go as far as making animal sacrifices and in some extreme situations human sacrifices. Boys involved in Yahoo Plus are the reason human harvest business and ritual killings are prominent in the country especially in the certain parts of the nation. This is what engineers the increasing rate of kidnap and cases of missing persons. Those in the yahoo business and have been successful open a learning center of sort called the “HK” meaning Hustling Kingdom. Each HK comes with its own rules with the head called chairman who funds it and gets 50%-70% of every cash.

The thing of cybercrime initially started with few people involved in it but these days alot of youths especially students are neck- deep in it. The effect of yahoo can be it is like a disease that spreads fast with the wind. For them, seeing 18 year olds owning cars worth millions tends to wet their minds and the influence of peer pressure takes on their perspective. Some see internet fraud as a pathway to success in life, some hide under the guise of

taking back the wealth of their ancestors from the white man, while some are pushed into it by extreme poverty. But all these are not genuine excuses to warrant involvement in any form of financial crime (economicconfidential.com).

2.2 Rate of Students' Involvement in Cybercrime

The findings showed that students are involved in cybercrime in many areas such as; cyber stalking, email hacking, phishing, encrypting of files, online spam sending; floatation of illegal business proposal; cybercrime with direct contact through phone; as so on (Amini-Philips, 2018). The students have in one way or the other been involved in cybercrime. Ngozi (2016) reported that the quest for money has made Nigerian youths to deeply involve themselves in cybercrime. She further found out that most of these students are deeply in cybercrime alongside their contemporaries. Denga (2011) in his own study disagreed completely the findings of Ngozi, stated that undergraduates are fully occupied with academic and vocational activities that can make them associate with cyber theft. Ben (2017) in his study reported that up to 90% of undergraduate students are very much involve in cybercrime and its activities. Adanma (2017) as well vigorously disagreed with Ben, as she concluded that the level of undergraduate student involvement in cybercrime is still not fully ascertained. Odo & Odo (2015) investigated the extent of involvement in Cybercrime activities

among students' in tertiary institutions in Enugu state of Nigeria. Their findings showed that students of higher institutions in Enugu state are involved in cybercrime. It also showed that students' involvement in cybercrime is dependent on gender and Institution type.

2.3 Types of Cybercrime

Cybercrime ranges across a wide range of activities. It is quite vivid that cybercrime include different kinds of criminal activities that are done on the internet space (Mohsin, 2020). At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or individual (Dennis, 2019). Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as fraud, trafficking in child pornography, digital piracy, money laundering, and counterfeiting.

2.3.1 Cybercrime on the Banking Sector

The life wire of the banking sector is the internet. Banks all over the Nigeria are introducing opportunities brought about by e-banking which is believed to have started in the early 1980's (Shandilya, 2011). Cybercriminals take hold of this opportunity to defraud banks and bank customers.

ATM fraud: In recent years, there has been widespread of ATM fraud across the globe (Jain, 2017). Through the automated teller machine (ATM) many people now get cash. In order to access an account, a user supplies a card and personal identification number (PIN). Criminals have developed means to intercept both the data on the card's magnetic strip as well as the user's PIN. In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual's account (Dennis, 2019). The number of ATM fraud has continued to increase due to negligence in the handling of ATM cards by bank customers. Most bank customers compromise their bank account details including their personal identification number to fraudsters (Jain, 2017).

Phishing: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorised businesses and financial institutions that are victim-ized (Wada). Phishing scams are wide range and greatly increasing. It has become one of the fastest growing cybercrimes in Nigeria. In Nigeria, bank customers usually fall victims**.**

Advance fee fraud: This is where Nigerian fraudsters obtain money fraudulently from some foreign nationals, mostly Americans, on the promise of getting married to them or an oil contract. These fraudsters extort money from their victims, promising to be in love with them and

agree to marry them and in the process demand for money in which they will use to travel and meet them abroad. Thus, many desperate foreigners seeking for quick means of making money or looking for spouse become victims of these cyber fraudsters (Martins, 2016).

Cyber-laundering: Cybercrime that comprises financial transactions using funds from criminal activities. Cyber laundering is based on e-payments, digital money and illegal hardcash that is converted to illegal e-money.

2.3.2 Cybercrime on Social Media Sector

Perlmutter (2019) opined that social media has become part and parcel of people's lives. Cybercriminals also make use of social networking sites like Twitter, Facebook, Instagram to lure them into scam.

Online charity: Here, the fraudster sends e-mails to their victims soliciting for funds and assistance to charitable organization that do not exist. Such scam contains emotional and touching messages aimed at appealing to the conscience of their victims.

Cyberbullying/stalking and blackmailing Scams: This involves the use of communication technologies to harass people. Some forms include cyber extortion, distribution of embarrassing pictures, delivery of threatening messages, cyberbashing to mock people and impersonating victims (Sabillon, Cano, Cavaller and Serra, 2016).

Prohibited/Illegal Content: This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Social Hijacking: This involves holding unto someone's social media account in exchange for money. The social media hijacker demands for money to release the person social media. Celebrities are usually victims of this crime some even go the extra length.

2.3.3 Cybercrimes in the E-Commerce Sector

The online market for buying and selling is constantly under threat by cybercriminals. E-commerce refers to the use of technology, particularly the Internet, to buy, sell and market goods and services to customers (Michael, 2014). These are some of the firms of cybercrime that threaten the e-commerce sector.

Illegal e-lotteries: The effort to get rich quickly by most Nigerians especially the students is often exploited by cyber fraudsters who send all kinds of tempting messages of an existing lottery bonanza where participants can be deceive with all sorts of items and money ranging from

cars, electronics, laptops etc. this form of cybercrime is rampant in Nigeria (Martins, 2016). Even the American visa lotteries have been used to lure many Nigerians to their doom as lots of student are eager to study abroad and these scammers are aware of this, and they respond by creating online visa lotteries to rip off unsuspecting students.

Sales Fraud & Forgery: In Nigeria, fraudulent sales of products that do not exist or that are replicas are increasingly rampant. The purchase of a good or good before actually seeing it has created ways for fraudsters to make dupe people through ads of fake products or in some cases, the total absence of the product. Many persons have fallen victim of this particular crimes on popular e-commerce websites.

Data and Airtime Time (DAT) theft from service providers: This is a reoccurring scam among the youths of today. They illegally gain access to "Cheat codes" and illegally use them to access unlimited data and airtime without paying for service.

2.4 Causes of Students' Involvement in Cyber Crimes

The motivation to commit crime and the supply of offenders tend to be at constant increase in contemporary society (Idom and Tormusa, 2016). The root implications of cybercrimes are not far-fetched. One only has to take a quick glance around the society to observe illicit wealth acquisition and its display. This is coupled with the fact that; the perpetrators are highly

exalted (Akwara et al., 2013). The problem is made worse by the high youth unemployment, the absence of enforceable prohibitive laws and the general laissez faire attitude of individuals and businesses regarding cyber security. Studies have shown the causes of cybercrime (Otuya, 2022; Adewole, 2021;Odita, 2019;Esere et al., 2017;Okeshola & Adeta, 2013;Ojedokun & Eraye, 2012;Tade & Aliyu, 2011). Hassan et al. (2012) identified urbanization, high unemployment, quest for wealth, poor implementation of cybercrime laws, inadequately equipped law enforcement agencies, and negative role models as some of the causes of proliferated cybercrimes by students in Nigeria.

Unemployment: Unemployment rate in Nigeria is high and stood at 23.1% in the fourth quarter of 2018. According to Okafor (2011), high unemployment in Nigeria comes with socioeconomic, political and psychological implication. It is known that over 20million graduate in the country do not have gainful employment (Omodunbi et al 2016). Over 5 million Nigerian university undergraduates have no hope of gainful employment when they graduate from the university. Hence, they resort to internet fraud as a means of paving ways for a source of livelihood and this automatically increases student involvement in cybercrime.

Corruption: Nigeria has continued to occupy a dominant place in the global ranking for corruption. In 2018, Nigeria was ranked the 144th most

corrupt nation in the world out of 176 countries (Transparency International, 2017). Corruption has eaten deep into the system. From the individual to organisational and institutional level including tertiary institutions. Even some the law enforcement agent are very corrupt that they collect bribe from these fraudsters.

Poverty and socio economic status of households: The spread of poverty and socio economic status is one of the main causes of internet fraud in Nigeria among students (Ayantokun, 2016). Nigeria is said to be living below the poverty line (below $1 per day). Adejoh, Alabi, Adisa and Emezie (2019) reported that 71% of Nigerian households are poor with the halving of this classified as extremely poor. In this scenario many parents that do not hold moral strongly will not mind when there their child starts making money no being bordered about the source of wealth. All they know is that someone has come to rescue them from poverty.

Peer Pressure: No man is an island and dome people can be influenced by their peers (Ojedokun & Eraye, 2012; Tade & Aliyu, 2011). Students are literarily usually faced with peer pressure on a daily. The oppression by yahoo boys on other student is not an exception. Yahoo student come to class with flashy wears, flashy cars and even discuss about their big spending among their peers and in no time influence their contemporaries to join in their illegal dealings. Everyone wants to belong to a certain group

or upper class without consideration of his / her background. They want to be like their friends hence they delve into cybercrime without giving regard to the effect they see it as “the ends justify the means”(Aghatise, 2006).

Negative role model/Influence Social media and entertainment sector: in 2007, a young Nigerian musician, Olumide Adegbolu (also known as Olu Maintain) released a hit song called “Yahooze”. The song, which sparked a lot of controversies, speaks of a flashy and expensive lifestyle. The funny thing is that these people are many students role models and since students are social media savvy they see these role models flaunt ill-gotten wealth on social media and even sing about them to the extent that they see it as the 'IN- THING" at in little time they join the bandwagon. In the last two year series of song that directly and indirectly advocate for the prominence of cybercrime have been top the Nigerian music chart likes of cash out by bella shurmda, Elon musk boys by Shallipopi.

Poor Implementation of Cybercrime Laws and Inadequately Equipped Law Enforcement Agencies: According to Laura (2011), African countries have received strong criticism for being unable to handle issues of cybercrimes due to inadequate infrastructure and inadequacy on the part of Law Enforcement Agencies. There are no tech devices that can forensically track down cyber criminals. Sometimes they make certain laws yet they fail execute them. Well, it not a new phenomenon because Nigeria is notorious

for having the best laws on paper without fully implementing it. It is worth noting that law enforcement agencies in Nigeria such as the EFCC and ICPC have been successful to an extent. Nevertheless, there is still room for improvement (Okafor, 2011).

Quest for wealth: Mere instinct shows that quests for wealth is another cause of cybercrimes in Nigeria. For any business to succeed, it is expected that, the rate of returns on the investment grow at a geometric rate, with minimal risk something that requires time, hardworking and process. Cyber criminals desire to invest minimal capital in a conducive environment that would reap maximum gains as they strive to become rich using the quickest means possible. Students of nowadays are not ready to lower their head and learn and use the knowledge to create something out of their ability but rather prefer the get rich quick means. They become greedy hence the try level up with their rich counterparts through cybercrime some even going the extent of going spiritual to aid their fraudulent activities. Studies have shown.

Societal emphasis on materialism: The society in itself constitutes it's own problem. Individuals and group in the society place emphasis on wealth without carefully getting to find out the source of wealth. It is not unusual to hear of people with questionable character and wealth being celebrated in society. Perpetrators make illegal money are celebrated by

people, resulting in an increasing justification for illegality (Adeniran, 2008; Ninalowo, 2016). This misguided disposition towards wealth gives the legal ground for the young to delve into cybercrime.

2.5 Implications of Cybercrime

The discovery of social media has brought about the awareness of cybercrime which has greatly increased students involvement in cybercrime, yearning to flaunt a lavished lifestyle not knowing the implications at stake (Ogunjobi, 2020). . Cybercrimes, whether 'yahoo yahoo' or 'yahoo plus' among students, has implications on the students, community and society (nation) at large.

Cybercrimes Implications on the Nigerian Economy

The implication of cybercrime has been, and is still being felt by all governments and economies that are connected to the Internet. Criminals uses the Internet, computers and other digital devices to facilitate their illegal activities as long as the financial gains outweigh the consequences when caught (Olusola, Samson, Semiu and Yinka, 2013). Cybercrime has developed into a new form of crime and also exist in Nigeria tertiary institutions which are now denting and drilling holes in the economy of the nation (Domes, 2014). Knowing about the quantity of Cybercrime as well as the economic impact is vital for both governments as well as businesses which could be a necessary tool to adjust the legal and regulatory

frameworks as well as institutional capacities. According to Vladimir (2005) internet is a wide range of interconnected network but it is now been used for criminal purposes due to the economic factors. Nigeria a third world country is faced with so many economic challenges such as poverty, corruption, unemployment amongst others, thereby, making this crime thrive. According to the Nigerian Communication Commission (2016), cybercrime and espionage cost the global economy upwards of 500bn annually and are the main contributors for dragging down economic growth across the world. A study by the security firm McAfee and the Centre for Strategic and International Studies (CSIC) revealed that the US, the world's largest economy loses about $100bn (€76bn, £65bn) from cybercrimes and espionage, including loss of key business data and intellectual property (Mathew, 2014). According to the PTI Contents (2009), over 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy. According to Abimbola (2013), cybercrime impedes the country's socioeconomic growth because it fosters a lack of trust and faith in profitable transactions, encourages the denial of

innocent Nigerians opportunities abroad, and results in job losses and revenue loss. Furthermore, it drives away foreign investors due to the low level of trust (Maitanmi et al 2013).

Cybercrimes Implications on the Nigerian Educational Sector

Societies all through time have always relied on the education for guidance (Ozturk, 2008). Chimombo (2015) postulates that education has always served to cultivate the innovative capabilities of individuals in a society and this has created opportunities for improvements in the economic, political, societal and moral outlook of individuals in a nation. Nations seeking to stimulate national development have invested in education (Ozturk, 2008). However, it is imperative to note that the Nigerian educational system has face terrible challenges occasioned by cybercriminals. These activities have negatively impacted on the advancement of the nation's educational sector (Ololube, 2016). Nwaokugha and Ezeugwu (2017) highlighted that student involvement in cybercrime activities in the educational sector negatively impacts social equality, merit and competence as it becomes rampant in the school campus. They further observed that these criminal acts in the educational sector has drained original intention of what the school ought to offer. The tertiary institutions have been metamorphosed to a citadel for acquisition of illegal 'yahoo' knowledge (Inaolaji, 2022). It has brought about lack of creativity, redundancy in acquisition of knowledge, lack of

drive to study, etc. Student have now shifted their focus from learning with the internet to making ill money with the internet thereby affecting their academic performance that some even drop out of school (Warner 2011, Igba and Nwambam, 2018).

Cybercrime Implications on the Reputational and Security of the Country

According to Oyebade (2019), the effect of the cybercrime acts among students is that it deters the reputation of the student, parent, community, and nation as a whole. In the case of yahoo plus people use body parts to get diabolical power hence citizens security becomes tampered with. At this international level. The country has been liable corrupt and criminal concentrated even when we have alot of individuals that are not into cybercrime. The fast rising involvement of students in cybercrime is leading to a situation where the reputation of the country is rub in the mud.

2.6 Measures to Curbing Student's Involvement in Cyber Crime

Prevention is always better than cure. Certain measures should be taken that would reduce students involvement in cybercrime.

Education and Sensitization: There should be campaign of NGOs against cybercrime. They should educate and sensitized students on the effects of cybercrime in order to curb it.

Establishment of Programs and IT Forums for Nigerian Students: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should set up IT laboratories/forum where students could come together to learn and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

Cyber Ethics and Cyber Legislation Laws: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cybercrimes will reduce. Security software like antiviruses and anti-spywares should be installed on all computers, in order to remain secure from cybercrimes (Laura, 2011). Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious program.

Execution and prosecution of offenders: It is one thing to say and it is another thing to do. Cybercriminals should be punished accordingly. Corrupt law enforcement agents should be removed from the system in order to ensure a transparent system

Job Creation and Skill Acquisition: Government should create job opportunities and also encourage small scale industry by giving them soft

loans and making favourable conducive policies like incentives, reduce taxes and so on. They should also encourage learning of new skills such as tailoring, hair styling, catering and confectionery, furniture making etc. This will go a long way in engaging them and creating a brighter future for the young.

In conclusion, Nigeria as a country is being regarded as a ridicule due to high rate of corrupt practices whose one example is cyber-crime activities. These criminal activities bring about reputation loss to a nation, financial loss, low productivity, etc. And these consequences are glaring in Nigeria. We must take action to combat Cybercrime through increased awareness and preventative measures.

2.7 Theoretical Framework

The study adopts the differential association theory and at the same time adopts the social strain theory.

Social differential theory was propounded by E. Sutherland. This theory focuses on how individuals learn to become criminals. The theory describes how ones environment influences one to delve into crime. Sutherland had developed the idea of the "self" as a social construct, as when a person's self-image is a reflection of interacting with other people. People learn delinquent behaviour as through association, as they pursue their profession (Tarde, 1912).The theory is influenced by the symbolic interactions

perspective (William's and McShane, 2013). In learning behaviour, the influence of the significant others (father, mother, sibling, close friends) outweighs the influence of generalised other (Sigel and Welsh, 2012).

The theory has the following assumptions:

1. Criminal behaviour is learned. Edwin Sutherland opined that there is nothing like a born criminal rather criminal behavior is learned.
2. Criminal behaviour is learned in interaction with other persons in the process of communication.
3. The principal part of the learning of criminal behaviour occurs within intimate personal groups.
4. When criminal behavior is learned, the learning involves both the method of committing the crime, and the specific direction of motives, drives, rationalizations, and attitudes.
5. The specific direction of motives and drives is learned from definitions of the legal codes as favorable or unfavorable.

The Second theory which is the social strain theory propounded by Robert k. Merton is an offshoot of Emile Durkheims 'anomie theory'. Social Strain theory explains that crime occurs as society puts pressure on individuals to achieve socially accepted goals, even though they lack the means to do so; hence individuals according to this theory are likely to commit crime. Robert K Merton highlighted five (5) types of individuals the conformists,

the ritualists, innovators, retreatists and rebels. For the course of the research emphasis will be placed on the innovators since accept the goals at the expense of the institutionalized means thereby using conventional means to achieve their goals. They construct new system through which they cope with the resultant frustration, strain, anger, and anxiety, pressure (Dearden et al., 2021).

2.7.1 Application of the Theory

Differential Association Theory

The theory can be reflected or used to explain the concentrated involvement of students especially those from poor backgrounds. The principle idea of Edwin Sutherland's differential association theory is that criminal behavior is learned from intimate groups, e.g. family members, relatives and friends.

Among peer groups discussion on wealth is very prominent. Most times the situation of poverty and negative circumstances surrounding ones environment forms a motivation or drive to do anything by all means to become wealthy. Since the influence of the significant others his very strong on the individual, the individual can be tune/influence by the parents, relatives etc. to delve into cybercrime. One of the assumptions of differential association theory is that the person's definition of crime is based on the legal codes of what is seen as favourable or unfavourable. In some certain homes today, cybercrime is a norm like it is not seen as crime

because some have justified the means as a way of collecting back what the Europeans collect from us during imperialism and colonial era especially they benefit from it for example, a young boy that stays in the core part of Benin where he has fellow students that are into crime and helped his parents out of poverty, buy cars for them ,built an expensive mansion, going on trips abroad and all than may be lured his own parents who want to also enjoy all these dividends by instigate them to same as his mate foregoing the consequences.

Social Strain Theory (Innovation)

This can be reflected in explain the involvement of students in cybercrime. Deviant behaviour or criminal behaviour is caused as a result of the dysfunction in the functioning of social systems/institutions. In a situation where by the system is not working out or there in instability in the social system, dysfunction is very bound to occur.

Innovation or innovator is an individual that creates a means out of/different from the institutionalized means to get the institutionalized goal. In a proper system that works, Education is a very key tool and qualification to achieving great things. In a system that actual works, one ought to go to school, acquire great knowledge and then with good as average result one ought to get a good paying job where his/her knowledge will be put to use. But this not the case in Nigeria, in Nigeria, being a

graduate with good result does not guarantee you a good job rather connection, corruption and negligence is what plays at the top. We have alot of sound student and graduate who are underemployed or worst still unemployed and these people are to eat,, put food on the table, are to breadwinners for their families, are to show evidence for their years and years of hardwork. In a situation where self-actualization seems blurred, students will device an alternative means which is out of the normal/institutionalized means to achieve the American dream (have the basic necessities of life, car, house, education, etc.).

SECTION THREE

RESEARCH METHODOLOGY

This chapter is thematically structured into six parts; research design, area of study, population of the study, sample size and sampling techniques, instrument of data collection, method of data collection and method of data analysis.

3.1 Research Design

This is the blueprint of the research work which gives a glimpse of the method adopted in the research process. It describes the process of how the research was conducted scientifically. The type of research used is the survey research design.

This type of research was preferred for the study because of the large population involved which cannot be studied without selecting a particular sample size that will serve as a representative of the entire population.

3.2 Area of Study

The study was conducted in the University of Benin (UNIBEN) which is the only Federal University in Edo State, Nigeria. The University which was established in 1970 houses two campuses; Ugbowo and Ekenwuan Campus which houses 77,000 students with about 14 departments. The

main campus is situated at Ugbowo, in the Ovia North East Local Government Area.

3.3 Population of Study

The total population of study is the total population of the student in University of Benin (UNIBEN). The total population of the university is about 77,000. Meanwhile the targeted population was choosen randomly student from different the faculties according to the sample size.

3.4 Sampling Size and Sampling Technique

Given the inability of the researcher to reach the entire populace due to limited time available for carrying out research and also due to the fact that it is a self-sponsored research work hence available finance has to be utilized diligently.

The sample size for this study was determined by adopting the Nassiuma (2000) formula:

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

Where n= sample size

N = Population of the study which is 77000

CV = coefficient of variation (take 0.5)

e = tolerance of desired level of confidence take 0.5 at 95% level

1 = constant

Therefore, the sample size for the University of Benin will be calculated as:

$$n = \frac{77000(0.5)^2}{0.5^2+(77000-1)0.05^2}$$

$$n = \frac{77000(0.25)}{0.25+(76999)0.0025}$$

$$n = \frac{192.7475}{192.7475}$$

n = 99.872

n = 100

n = 100 (this means that the study sample size of university of Benin is 100).

3.5 Instruments for Data Collection

The research made use of questionnaire.

Questionnaire Title: Implication of Cybercrime among Students in the University of Benin

The questionnaire was divided into two (2) sections.

Section A – Demographic. This consist of information relating to the demographic characteristics of respondents. It is the big-data of respondent like sex, age, ethnic group etc.

Section B – This contain vital information and data concerning the topic of research. The section consist of close and open ended questions designed to elicit responses appropriate to analysis.

Using the closed open ended questionnaire will be for two reasons. Firstly to cover vast number of persons in the short time frame. Secondly, some persons will want to discuss the reason for their answer or opinion hence the reason for the openness of the questionnaire.

3.6 Method of Data Collection

The study adopted quantitative techniques for data collection. The quantitative method is the use of questionnaires.

3.7 Method of Data Analysis

The data collected for the study was analyzed using the several method. The researcher will make use of frequency table and percentage table in the analysis.

3.8 Limitation of study

The following were the obstacles encountered during the course of this study

a) Limited time constrain during the course of study

b) Financia constrain during the course of study

c) unwillingness for some of the respondent to give their opinions freely

SECTION FOUR

ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter presents the results and discussion of findings in line with the research questions. It is discussed under the sections of Questionnaire response rate, Analysis of demographic characteristics of the respondents, answering of research questions and discussion of findings

4.1 Response rate

A sample of 100 respondents was conveniently drawn from the 77,000 student population.

Table 4.1 Questionnaire Response Rate

Number of copies of Questionnaire Administered	Number of copies of Questionnaire Retrieved	Percentage of copies of Questionnaire Retrieved (%)
100	100	100

Table 4.1 shows the questionnaire response rate from the table, it was shown that a total of 100 copies of questionnaire were administered and retrieved from all the sampled respondents. From the analysis of the

questionnaire response rate, it is evident that the response rate of the respondents was high.

4.2 Demographic Characteristics of the Respondents

4.2.1 AGE DISCRIBUTION

AGE	FREQUENCY	PERCENTAGE (%)
16-20	36	36.0
21-25	44	44.0
26-30	14	14.0
31-35	6	6.0
36-40	0	6.0

FIG 1: BAR CHART DISTRIBUTION OF AGE DISCRIMINATION

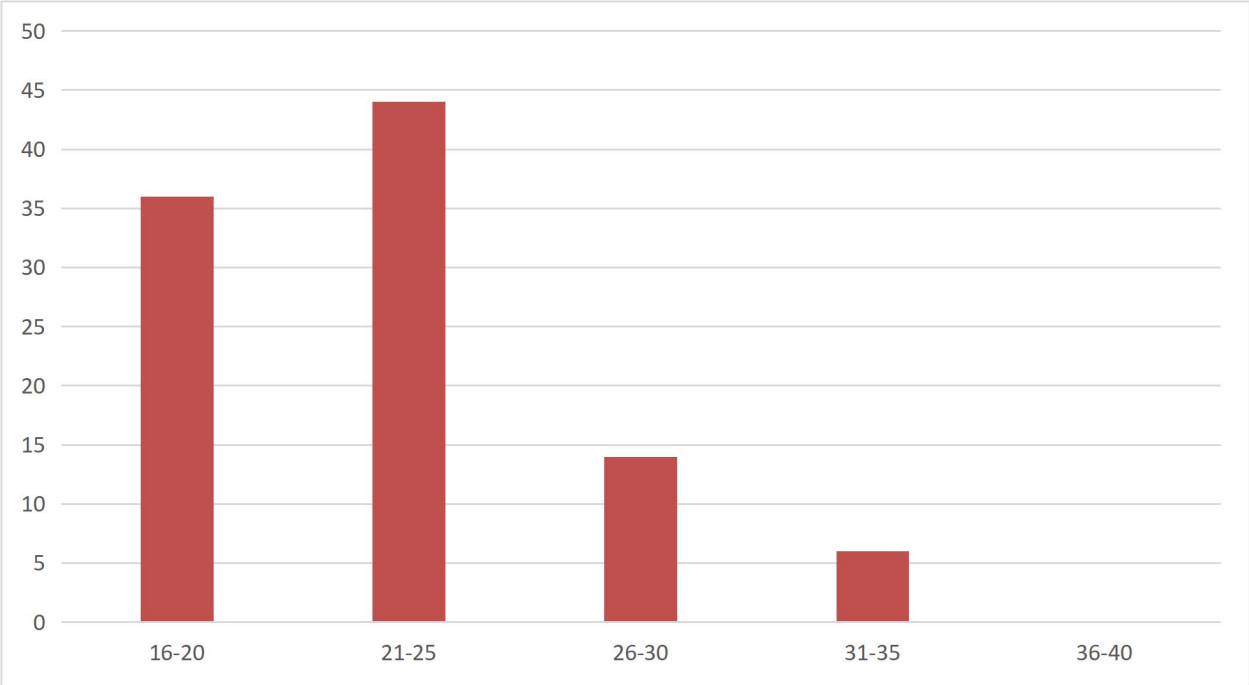

Table 4.2.1 Reveals the age range distribution of the respondents. Majority of the respondents in this study fall within 21 – 25 years old (44)

and represented 44% of the total respondents, while (36) belong to the 16 – 20 years age range and corresponds to 36% of the total respondents. This implies that majority of the respondents were within the 21– 25 years age bracket.

4.2.2 SEX DISTRIBUTION

SEX	FREQUENCY	PERCENTAGE (%)
MALE	40	40.0
FEMALE	60	60.0

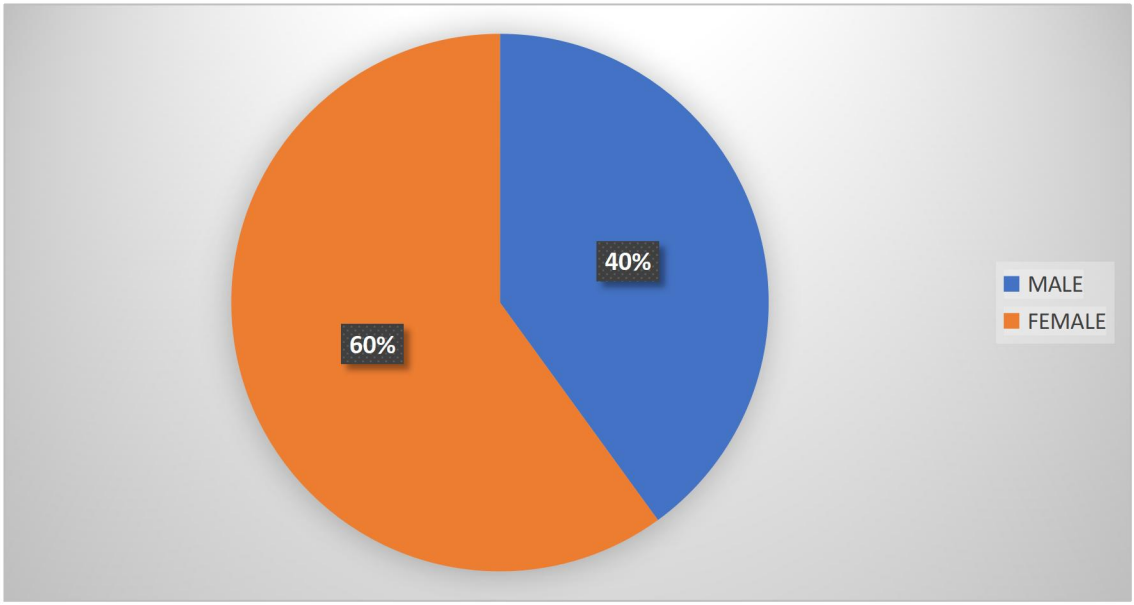

Table 4:3.2. Reveals the sex distribution of the respondents. Majority of the respondents in this study were female (60) and represented 60% of the total respondents, while 40 were male respondent with 40% of the total respondents. This implies that majority of the respondents were females.

4.2.3 Religious Distribution

RELIGION	FREQUENCY	PERCENTAGE (%)
CHRISTIANITY	92	92.0
ISLAM	8	8.0
AFRICAN TRADITIONAL RELIGION	0	0.0

FIG 3: BAR CHART DISTRIBUTION OF RELIGION

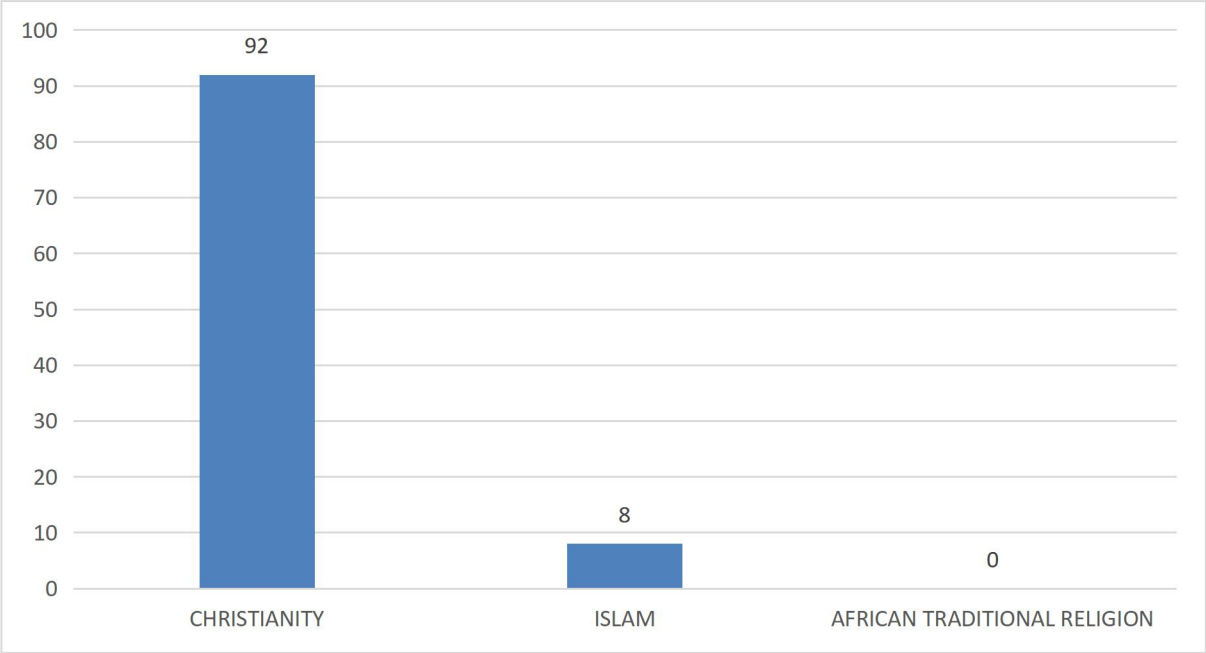

Table 4.2: Reveals religion distribution of the respondents. Majority of the respondents in this study were Christians (92) and represented 92.0% of the

total respondents, while Muslim (8) represented with 8.0% This implies that majority of the respondents were Christian.

4.2.4 FACULTY DISTRIBUTION

FACULTY	FREQUENCY	PERCENTAGE (%)
PHARMACY	6	6.0
ART	12	12.0
SOCIAL SCIENCE	18	18.0
ENVIRONMENTAL SCIENCE	4	4.0
AGRICULTURE	4	4.0
EDUCATION	8	8.0
LIFE SCIENCE	8	8.0
PHYSICAL SCIENCE	6	6.0
ENGINEERING	8	8.0
BASIC MEDICAL SCIENCES(BMS)	6	6.0
LAW	4	4.0
MANAGEMENT	8	8.0
School of medical science	4	4.0
School of Dentistry	4	4.0

FIG 4: BAR CHART DISTRIBUTION OF FACULTY DISTRIBUTION

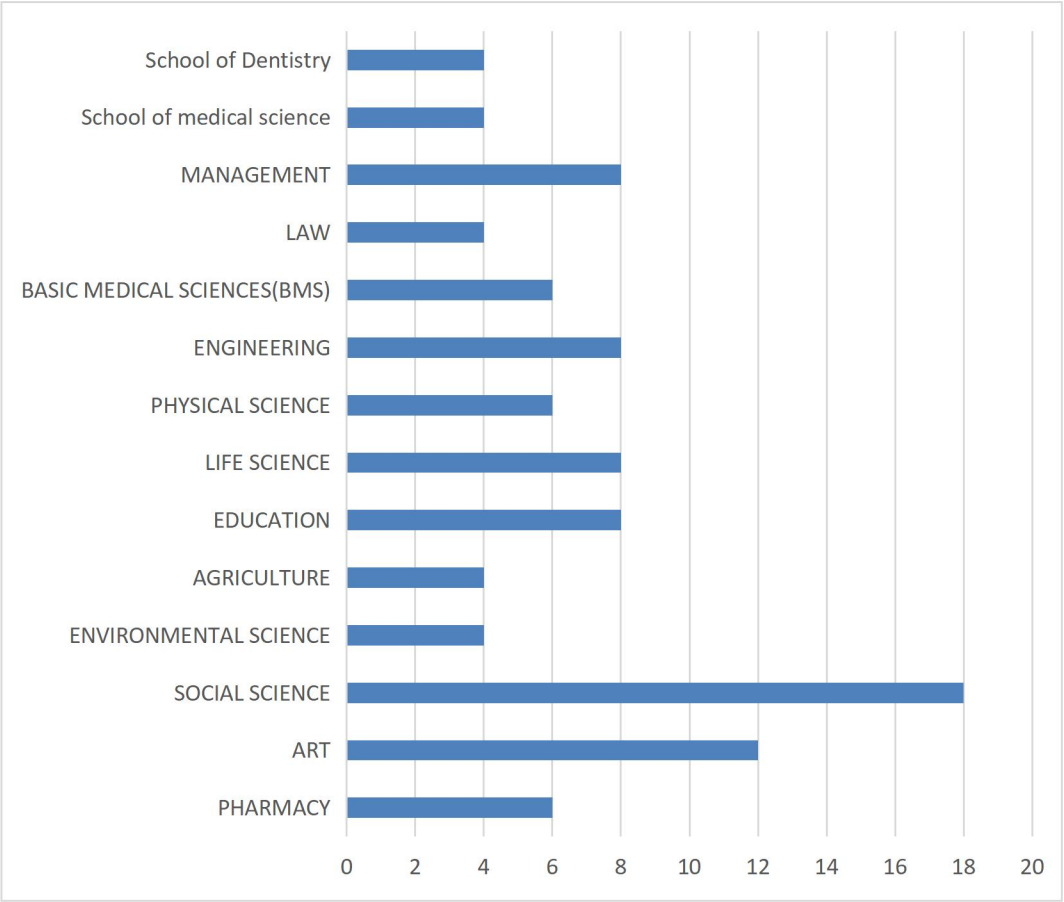

Table 4.2: Reveals faculty distribution of the respondents. Majority of the respondents in this study were students from facultyof social sciences (18) and represented 18.0% of the total respondents, whilerespondents from faculty of arts was 12%. Respondents from faculty of management science,life science engineering, education, were 8% each. While facultiy of pharmacy, physical science, BMS, all had 6% respondents each. This

implies that majority of respondents are from social science. Faculty of law, agriculture, environmental science, school of medical scienc, School of dentistry produced the least number of respondent with 4% each. This implying that faculty of social science had the highest number of respondent in the this research.

4.3 Answering Research Questions and Discussion of Findings

This section presents the analysis of the four research questions raised for this study.

Question 1: What is the rate of involvement in cybercrime amongst student in the University of Benin.

Items on the questionnaire that relates to research question one were analyzed as follows:

Table 4.3.1a

Question	Yes	No
Do you know what cybercrime is?	86 (86%)	14(14%)

Thematic analysis on respondents definitely of cybercrime:

Table 4.3.1b

Defrauding people of money through the internet	16(16%)
Use of computer to dupe an individual	6(6%)

Internet fraud	36(36%)
The use of computers, computer related devices ,website as well as apps to engage in criminal activity	16(16%)
The use of internet to bully,hijack,blackmail and collect money from individuals or companies	12(12%)

Table 4.3.1c

Common name	Frequency
Yahoo Yahoo	72(72%)
Internet/cyber fraud	16(16%)
419	4(4%)
Scam	4(4%)
G	4(4%)

Table 4.3.1d

PERCENTAGE range(%)	FREQUENCY
1-20	8(8%)
21-40	18(18%)
41-60	22(22%)
61-80	30(30%))
81-100	12(12%)
NIL	10(10%)

Table 4.3.1e

Statement	Yes	No	Nil
Do you think males are more involved in cybercrime than females	76(76%)	12(12%)	12(12%)

From 4.3.1a, it reveals that 86% of the respondents are aware of what cybercrime entails while 14% are not unaware. In table 4.3.1b, the 86 correspondent went further to give various definition of what cubercrime is. Out of the 86%, cybercrime was defined as defrauding people through the internet (16), the use of internet to dupe people (6), the highest recurring definition was defining cybercrime as internet/cyberfraud, The use of computers, computer related devices ,website as well as apps to engage in criminal activities(16),use of internet to bully,hijack,blackmail and collect money from individuals or companies(12).

Table 4.3.1c give analysis of the common namesfor cyber crime in Nigeria which are, yahoo yahoo(72%) , scam(4%) internet/cyber fraud(16%), 419(4%) and 'G'(4%). This reveals that yahoo yahoo is the most common term used to describe cybercrime in Nigerian. The analysis reveals tCybercrime socially tagged "yahoo yahoo boys" (Tade 2011 and Aliyu 2011).

Table 4.3.1d shows the percentage of student involved in cybercrime. Questionaires that had percentage in it, the average was used to determine the exact percentage (1-20)% with 8% , (21-40)% with 18%, (41-60)% with 22%, (61-80)% with 30%, (81-100)%.with 12% and 10percent of the correspondent with no reaponse at all. From the table, it is revesled that 61-80 percentage range had the highest hence we can say that student involvement in cybercrime is relatively high.). Cybercrime in largely

perpetuated by student in tertiary institutions (Tade 2011 and Aliyu 2011)This agree with Alemika(2007) when he agred that cybercrime has now become a norm ad the percentage of student involved in cybercrime is quite high ranging above the average percentage of 50%

Table 4.3.1e reveals the rate on involvement in cybercrime amongst male and female in the University of Benin. 76% agree that males are more involved in cybercrime while 12% of the respondent disagree meanwhile 12% gave no response at all. This agrees with Odo & Odo (2015) that cybercrime is also dependent on gender (sex). This may be due to idea that men are more of economic providers than women hence tge phobia for not being economically successfull may lure this young men to cybercrime.

Question 2: What are the forms/types of cybercrime practiced by student in the University of Benin

Table 4.3.2a

Question	Yes	No	Nil
Have you been a victim of cybercrime	32(32%)	64(64%)	4(4%)

Table 4.3.2b

Types/forms	Frequency
ATM FRAUD	4(4%)
Cyberbullying and blackmailing	1(1%)
E-lottery theft	6(6%)
Money Laundering	3(3%)

Social hijacking	4(7%)
Sales fraud and fraudery	6(6%)
Data and airtime theft	7(7%)
Illegal content	1(1%)
Total	32(32%)

Table 4.3.2a shows the number of respondents that have been victims of cybercrime. With 32% being victims of cybercrime? 64% have never been direct cictims of cybercrime. Meanwhile 2% gave no response at all. From of the above analysis, it is revealed that alot of student have bot been victims cybercrime which implies that stident victimization to cybercrime is exaggerated and give the probability that most victims of Cybercrime maybe foreigners or uneducated people.

Table 4.3.2. The respondents 32persons who have been victims of cybercrime went further to tuck the various forms of cybercrime thave been victims to. ATM Fraud(4%) , cyberbullying and blackmailing(1%), E-lottery theft(6%), money laundering, (3%) social hijacking(4%), sales fraud and forgery(6%), data/ airtime theft(7%), illegal content (1%). From the above analysis it isc quite vivid that illegal e-lotteries is one of the rampant cybercrime people fall victim of (Martins, 2016)

Question 3: What are the possible causes of cybercrime among student in University of Benin

Thematic analysis of the causes of cybercrime

Table 4.3.3a

Themes	FREQUENCY
Poverty	42(42%)
Greed	16(16%)
Peer pressure	26(26%)
Luxury lifestyle/get rich quick syndrome	4(4%)
Unemployment	4(4%)

Table 4.3.3b

Question	Yes	No	Nil
Do you think peer pressure is a major influencer to cybercrime	78(78%)	20(20%)	2(2%)

Table 4.3.3c

Question	Yes	No	Nil
Do you think family background is a major influencer to cybercrime	68(68%)	30(30%)	2(2%)

Table 4.3.3d

Question	Yes	No	Nil
Do you think cybercrime is justifiable	26(26%)	68(68%)	6(6%)

Thematic analysis for whether cybercrime is justifiable or not

Table 4.3.3d

No(not justifiable because)	It is wrong and illegal	32(32%)
	It's building on others hard work	18(18%)
	its an addiction	3(3%)
	It's bad for reputation	5(5%)
	There are other legal means of making money	2(2%)
Yes(justifiable because)	everyone steals even those that make the law	4(4%)
	For survival and financial Freedom	14(14%)
Nil		22(22%)

Analysis and Discussion for Question 3

From the above table we see that we have the response of respondents in table 4. We see that thhighest cause of cybercrime is poverty which carries the response rate of 42%, followed by peer pressure carrying the response rate of 26%. Others are Greed(16%),luxury lifestyle/get rich quick syndrome (4%), unemployment (4%). According to Ayantokun(2016),

poverty and asocio economic status is one of the main causes of cyber and this analysis attest to the fact.

In table 4.3.3b We see the correspondent were asked if they think peer pressure is one of the major influencers to cybercrime and we got 78% positive responses and 20% negative. Meanwhile we had 2% of the respondent making no.attempt to the this particular question.The power of peer pressure cannot be underrated as No man is an island and some people can be influenced by their peers (Ojedokun & Eraye, 2012; Tade & Aliyu, 2011)

In table 4.3.3c We see the correspondent we asked if they think family background is a major influencer to cybercrime we had 68% positive response and 30% negative. Meanwhile we had 2% of the respondent making no attempt to this particular question.

In table 4.3.3d It analyses whether if is cybercrime is justifiable or not . 26% of the correspondent opined that cybercrime is justifiable while 68% opined that is is not justifiable. Meanwhile 6% did not give an answer.

In table 4.3.3e it further explains the various reasons why it is justifiable or not. For those that said it justifiable they gave reasons such as the fact that everyone steals (4%), second reason why it is justifiable is because of the need for survival and financial Freedom (14%). For those that gave the opined that cybercrime is not justifiable, they gave reasons such as; it is

wrong/illegal(32%), it building on other hardwork(18%),it is an addiction(3%),it is bad for reputation (5%), there are other means of making money(2%)

Question 4:implications of cybercrime among student in the university of Benin (main objective question)

Thematic analysis of the implications of cybercrime amongst students in University of Benin

Table 4.2.4a

Jail term	18(18%)
Socio economic degradation	14(14%)
Academic unseriousness	12(12%)
Reduce student creativity because they become dependent on yahoo	9(9%)
Brings about bad reputation which hinders foreign investment	16(16%)
Financial freedom (p0ositive short term implication)	7(7%)
Nil	24(24%)

Table 4.2.4b

Question	Yes	No	Nil
Do you think the involvement of student in cybercrime is so strong that it cannot br correct	44(44%)	54(54%)	2(2%)

Table 4.2.4c

Question	Yes	No	Nil
With the involvement of student in cybercrime, do you think there is hope for the future of Nigeria	78(78%)	20(20%)	2(2%)

Analysis and Discussion for Question 4

Table 4.3.4a reveals the various implications of cybercrime which are jail term(18%), ,socio economic degradation(14%), academic unseriousness (12%), reduce student entrepreneurial creativity(9%), bad reputation which hinders foreign investment(16%) , financial Freedom(7%) which gears toward positive impact. Meanwhile 24% gave no response..The analysis agrees with reveals the fact that student involvement in cybercrime affects academic performance (Warner 2011, Igba and Nwambam, 2018). it also drives away foreign investors due to the low level of trust (Maitanmi et al 2013).

Table 4.2.4b revealed the number of respondent that see that thr issue of student cannot be coorected as 44% while 54% gave a negative answer to the question. Meanwhile 2% gave no response at all

Table 4.3.4c reveals the 78% believe that there is hope for Nigerians despite student involvement in cybercrime while 20% do not have hope in Nigeria . Meanwhile 2% gave no response.

Question 5: What are the possible solutions ro cybercrime amongst students in the University of Benin

Table 4.2.5a

Question	Yes	No
Do you think there are remedies to cybercrime amongst student in the University of Benin	54(54%)	46(46%)

Thematic analysis of the possible solutions to cybercrime amongst students in University of Benin

Table 4.2.5b

Sensitization and Enlightenment on the negative impact of cybercrime	22(22%)	
Job creation and skill acquisition	18(18%)	
Established and proper enforcement of cybercrime laws	8(8%)	
Reduce cost of living and aid student through their education by giving them incentives	6(6%)	
Total	54(54%)	

Analysis and Discussion for Question 5

Table 4.2.5a reveals that 54% opined that there are possible remedies to cybercrime, 46% opined that there are no remedies to cybercrime.

Table 4.2.5b . The 54 responds that replied positive to the question on if there are possible remedies went further to reveal various possible remedies to cybercrime which are: sensitization and Enlightenment on the negative impact of cybercrime(22%), job creation and skill acquisition (18%), establishment and proper law enforcement of cybercrime laws(8%), reduce cost of living and aid student through their education by giving them incentives(6%).

SECTION FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This study examined the implication of cybercrime amongst students in the University of Benin. The study reviewed related literature from other authors on the subject matter. A sample of 100 student from the prestigious university of Benin was drawn from the total population of 77000 student population. Four research questions and two hypotheses were formulated and analyzed in this study. A 100% response rate was obtained from the administered questionnaire. The data collected were analyzed thematically and using descriptive statistics such as frequency counts, percentages.

5.2 Conclusion

The study concluded that since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by students while using the internet which will assist in challenging this major threat Cybercrime. Therefore, the study reveals that there is significant influence of the implications of students' involvement in cybercrime on the educational sector of Nigeria. Also that there is significant influence of the implications of students'

involvement in cybercrime on the Nigeria economy. Respondents agreed to this fact through the survey done. Some opined that some see and cannot deny the obvious negative implication become sacrificial lamb in order for their family to survive and scale through their tertiary education

5.3 Recommendations

Based on the findings and conclusion;

1. There should be a more proactive approach that will allow law enforcement agencies to track and investigate students involve in cybercrime within and outside the institution. Besides, most of these students that practice such act can be easily tracked within their hostels in the institutions.
2. School management should be allow to report students detected to be involve in cybercrime as to averts its escalation, because by doing so will reduce the perpetration of cybercrime within the school. This can only be achieved through effective collaboration between school management and law enforcement agencies.
3. Federal and state government, as well as educational communities should intensify campaigns on cybercrime awareness among Nigerian undergraduate students in order to make them understand that cybercrime is a criminal offence punishable under the criminal act with

attendant adverse consequence of jeopardizing their educational accomplishment when convicted.

4. Seminars and skill acquisition centers should be created by the government to reduce unemployment rate.
5. Individuals should also play their part by avoiding any suspected fraudster alert like fake bank alert and also maintain privacy of any of their password in the internet.
6. Grants and loans should be given to individuals and small scale industries to direct their interests into working to earn a better living than being engaged in cyber-crimes.
7. Churches leaders, Muslims faithful and practitioners of African Traditional Religion should preach against illegal ways of making money to the adherents of their respective religions.
8. Parents should inculcate good moral values in the children that even when they grow up and live on their own as students in various tertiary institutions they will not be pressured to be a party to such criminal act.

BIBLIOGRAPHY

Abraham, N.M. (2011). Functional education, militancy and youth restiveness in Nigerias Niger Delta: The place of multi-national oil corporations (MNOCs). *African Journal of Political Science and International Relations, 5*(10), 442-447.

Adanma, J. (2017). Awareness level of undergraduate students and cybercrime among undergraduate students in South-East zone of Nigeria. Journal of Social Media Review, 5(3), 20-29.

Akpan, C. (2016). University students and cybercrime: An indispensable critical review. *Journal of Sociology, 2*(2), 181-186.

Akwara, A.F., Akwara, N.F, Enwuchola, J., Adekunle, M. & Udaw, J.E. (2013). Unemployment and poverty: Implications for national security and good governance in Nigeria. *International Journal of Public Administration and Management Research (IJPAMR), 2*(1).

Alemika, A.G. (2007). Some human dimensions of computer virus creation and infection. *International Journal of Human-Computer Studies, 52*(5), 899-913.

Amini-Philips, C. (2018). Awareness and involvement in cybercrime among undergraduate students in universities in Rivers State, Nigeria. *International Journal of Humanities and Social Science Invention (IJHSSI), 7*(3), 39-43.

Anah, B.H., Funmi, D.L. & Julius, M. (2013). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology.*

Asokhia, M.O. (2010). Enhancing national development and growth through combating cybercrime/internet fraud: A comparative approach. Institute of Education, Ambrose Alli University, Ekpoma, Edo State, Nigeria. *Social Sciences Review, 23*(1), 13-19.

Ayo, E. (2010). Convergence and policy issues in ICT sector. In G.O. Ajayi (Ed) *Proceedings of workshop on national information and communication infrastructure, policy, plans and strategies.* Abuja, Nigeria. 28-50.

Ben, F. (2017). Cybercrime awareness level of students: The media role. *Journal of Social Development, 4*(2), 92-101.

Bengal, S., Babatunde, S, & Bankable, F (2012). *Economic cost of cybercrime in Nigeria.*

Billy, H., Bradford, W.R. & Bonnie, S.F. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure to fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*.

Brenner, S.W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. London: Oxford University Press.

Brush, K., Rosencrance, L. & Cobb, M. (2020). Cybercrime. Available at: https://searchsecurity.techtarget.com/definition/cybercrime

Chiemeke, B.S. (2012). A security beget insecurity? Security and crime prevention awareness and fear of burglary among university students: The East Midlands. *Security Journal, 22*(1), 3-23.

Chimombo, J.P. (2005). Issues in basic education in developing countries: An exploration of policy options for improved delivery. *Journal of international cooperation in education, 8*(1), 129-152.

Denga, A. (2011). *Youths and cyber theft.* Lagos: Ademola Publishers

Domes, J.O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116-12.

Folashade, B.O. & Abimbola K.A. (2013). The nature, causes and consequences of cyber-crime in tertiary institutions in ZariaKaduna State, Nigeria. *American International Journal of Contemporary Research, 3*(9).

Gbadamosi, R.A. (2017). *Perception of cybercrime among Nigerian youths: A case study of Caritas University,* 5- 47.

Halder, D. & Karuppannan, J. (2011). *Cyber-crime and the victimization of women: Laws, rights and regulations.* IGI Global Publication.

Hassan, A.B., Lass F.D. & Makinde J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology, 2*(7), 626–631.

Igba, D.I., Elizabeth, C.I. & Aja, S.N. (2018). Examine cybercrime among university undergraduates: implications on their academic

achievement. *International Journal of Applied Engineering Research, 13*(2).

Inaolaji, O. (2022). Adverse effect of cybercrime on society and personality. Derived from business newspaper.

Jain, S. (2017). ATM frauds-detection & prevention. *International Journal of Advances in Electronics, 4*(10), 82-89.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south.* Hampshire: Palgrave Macmillan.

Laura, A. (2011). *Cyber-crime and national security: The role of the penal and procedural law research fellow.* Nigerian Institute of Advanced Legal Studies.

Maat, S. (2004). "Cybercrime: A comparative law analysis" (Doctoral thesis), University of South Africa, Pretoria, South Africa p.239.

Martin, L. (2016). *General introduction to cybercrime effects in Nigeria sector*. Retrieved from McLeod.

Mathew, J. (2014). Cybercrime cost global economy $500bn annually. *International Business Times* retrieved from: http://www.ibtimes.co.uk/cybercrime-csic-mcafee-hacking-493506

Meke, E.S.N. (2012). *Urbanization and cybercrime in Nigeria: Causes and consequences.*

Ndubueze, P. N. (2013). Social values and the yahoo boys' subculture in Nigeria: Towards a paradigm shift for national value re-orientation. *The Nigerian Journal of Sociology and Anthropology, 11*(1).

Ngozi, S. (2016). Students' perception of cybercrime and its implications. *Journal of Social Development, 4*(2), 50-57.

Nigeria Communication Commission (2016). A summary of the legislation of cybercrime in Nigeria. Retrieved on the 26th of July, 2016 from www.thecommunicatormagazine.com

Nwaokugha, D.O. & Ezeugwu, M.C. (2017). *Corruption in the education industry in Nigeria.*

Odom, A.I. & Odom, C.R. (2015). The extent of involvement in cybercrime activities among students' tertiary institution in Enugu State of

Nigeria. *Global Journal of Computer Science and Technology: H Information & Technology, 15*(3), 1-6.

Okesola, F.B. & Abimbola, K.A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State of Nigeria. *American International Journal of Contemporary Research 3*(9), 98-11

Oluwadare, C.T., Oluwasanmi, L.A. & Igbekoyi, K.E. (2018). *Prevalence and forms of cybercrime perpetrated by students in public tertiary institutions in Ekiti State*. Department of Sociology, Ekiti State University, Ado-Ekiti, Ekiti State.

Panda Security (2019). Types of cybercrime. Retrieved from: https://www.pandasecurity.com/ PTI Contents (2009). India: A major hub for cybercrime. Retrieved from: http://business.rediff.com/

Rishi, R., & Gupta, V. (2015). Strategic national measures to combat cybercrime: Perspective and learning for India. Retrieved from http://www.ey.com/Publication/ vwLUAssets/ey-strategic-national-measures-to-combat-cybercrime/$FILE/ey-strategicnational-measures-to-combat-cybe

Sabillon, R., Cano, J., Cavaller, V. & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165–176.

Tade, O. & Aliyu, I. (2011). Social organisation of cybercrime amongst University students in Nigeria. *International Journal of Cyber Criminology*.

The Internet Crime Compliant Centre (2012). 2012 Internet Crime Report. Internet Crime Compliant Centre. Retrieved from: https://www.ic3.gov

Thomas, J.H. (2013). *Cybercrime and criminological theory: Fundamental readings on hacking, piracy, theft, and harassment, (first edition).*

APPENDIX

DEPARTMENT OF SOCIOLOGY AND ANTHROPOLOGY
FACULTY OF SOCIAL SCIENCES
UNIVERSITY OF BENIN
BENIN CITY

QUESTIONNAIRE ON
IMPLICATIONS OF CYBERCRIME AMONGST STUDENTS IN UNIVERSITY OF BENIN, BENIN CITY

Dear Respondents,

REQUEST FOR COMPLETION OF A RESEARCH QUESTIONNAIRE

I am final year student of the above department and institution. As part of the requirement for my B.Sc. degree, I am conducting a research work on "Implications of cybercrime amongst students in University of Benin, Benin City".

I humbly request you to validate this research instrument by responding to the items, ticking your response in the spaces provided below. Your response will be treated with strict confidentiality and used for academic purpose only.

Thanks for your anticipated co-operation.

Okey Esther Ceremi
Research Student

Instruction: Please tick (√) appropriately in the following section.

SESSION A: PERSONAL DATA OF THE RESPONDENT

- Age: 16 – 20 years [ ], 21 – 25 years [ ], 26 – 30 years [ ], 31 – 35 years [ ], 36 – 40 years [ ]
- Sex: Male [ ], Female [ ]
- Religion: Christianity [ ], Islam [ ], African Traditional Religion [ ]
- Faculty:_____

SESSION B: **RESEARCH QUESTIONS**

RATE OF STUDENTS INVOLVEMENT IN CYBERCRIME

- Do you know what cybercrime is? Yes [ ] No [ ]
- If yes, what is cybercrime? _____

- What is the common name for cybercrime in Nigeria? _____
- How many percent of student do you think are involved in cybercrime (both Yahoo and Yahoo plus). _____
- Do you think males are more involved in cybercrime than females? Yes [ ] No [ ]

TYPES/FORMS OF CYBERCRIME AMONG STUDENTS

- Have you been a victim of cybercrime? Yes [ ] No [ ]
- Which have you been a victim of? ATM fraud [ ] Cyberbullying [ ], E-lottery theft [ ], Money laundering [ ], Cyberbullying and blackmailing [ ], Social hijacking [ ], Sales fraud and forgery [ ], Data/airtime theft [ ], Illegal content [ ]

CAUSES OF CYBERCRIME AMONG STUDENTS

12.What do you think causes students to engage in cybercrime? _____

13.Do you think peer pressure is a major influencer to cybercrime? Yes [ ] No [ ]

14.Do you think family background is a major influencer to cybercrime? Yes [ ] No [ ]

15. Do you think that cybercrime is justifiable? Yes [ ] No [ ]

16.If Yes or No, explain _____

IMPLICATIONS OF CYBERCRIME AMONG STUDENTS

17.What do you think are the implications of cybercrime? _____

18.Do you think the involvement of students in cybercrime is so strong that it cannot be corrected? Yes [ ] No [ ]

19.With the involvement of student in cybercrime, do you think that there is hope for the future of Nigeria? Yes [ ] No [ ]

REMEDIES TO CYBERCRIME AMONG STUDENTS

20.Do you think there are remedies to cybercrime amongst students in University of Benin? Yes [ ] No [ ]

21.If Yes, what are the remedies? _____