IMPACT OF CYBERCRIME ON THE EDUCATIONAL PERFROMANCE OF STUDENTS OF SELECTED SECONDARY SCHOOLS IN IKPOBA OKHA LOCAL GOVERNMENT AREA, BENIN CITY, EDO STATE.

BY

NELSON UGWU

SSC1810114

THE DEPARTMENT OF SOCIAL WORK

FACULTY OF SOCIAL SCIENCES,

UNIVERSITY OF BENIN,

EDO STATE

OCTOBER 2023

IMPACT OF CYBERCRIME ON THE EDUCATIONAL PERFROMANCE OF STUDENTS OF SELECTED SECONDARY SCHOOLS IN IKPOBA OKHA LOCAL GOVERNMENT AREA, BENIN CITY, EDO STATE.

BY

NELSON UGWU

SSC1810114

BEING A PROJECT SUBMITTED TO THE DEPARTMENT OF SOCIAL WORK, FACULTY OF SOCIAL SCIENCES, UNIVERSITY OF BENIN, EDO STATE, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELORS OF SCIENCES (B.Sc) DEGREE IN SOCIAL WORK

OCTOBER 2023

CERTIFICATION

We certified that this project was carried out by **Nelson Ugwu** with the Matriculation Number: SSC1810109 of the Department of Social work, Faculty of Social Sciences, University of Benin, in the fulfilment of the requirements for the award of the degree of Bachelor of Science (B. Sc) in Social work.

_____ _____

Mr. P.A. Ugege **Date**

(Project Supervisor)

_____ _____

Dr. Sunday Ofili Ibobor **Date**

(Head of Department)

DEDICATION

This project is dedicated to the Lord Almighty, and to my lovely parents, for their unrelenting effort towards my academic success.

ACKNOWLEDGMENTS

My profound gratitude goes to God Almighty for his grace, favour and mercies upon my life and the great success achieved during my study in the University of Benin, could have not been visible without His grace and favour.

My profound gratitude goes to my supervisor Mr. P.A. Ugege for his patience, guidance and unwavering support have been the bedrock upon which this project was built, his expertise and willingness to invest time and energy into my development as a researcher have been invaluable, I am deeply appreciative of the mentorship I received throughout the journey.

I would also like to express my sincere appreciation to my dedicated lecturers, Dr. Kelly Imafidon, Dr. Owie Ukponahiusi, Dr. Sunny Omigie, Prof. Ugiagbe, who have played a crucial role in shaping my academic journey, throughout my coursework, their commitment to imparting knowledge, their passion for their respective fields, and their willingness to go the extra mile for their students have been inspiring, their lectures well not just lessons but gateways to new horizons of understanding and discovery.

My profound gratitude goes my family, I cannot express how much your unwavering financial, spiritual and moral support and belief in me have meant, my parents in particular, Mr. and Mrs. Ugwu have been a constant source of encouragement, and their sacrifices for my education will forever be etched in my heart, your belief in my potential has been a driving force, and I am profoundly grateful for your love and

support. My siblings, Mrs. Besty, Mrs. Lydia, Mr. Thomas, Mr. Samuel, Mrs Ifeoma, Mrs. Esther and to my in-laws Mr. Daniel, Mr. Kinsley, have been pillars of strength throughout this endeavor, their encouragement and understanding during the most challenging moments have been a source of solace and determination., their belief in my capabilities has been a constant source of inspiration.

I would like to express my sincere appreciation to my friend and course mate, Kelly Tawio, Iyore Eghe Nova, Honour, Jerry, Umoru, Courage, Kachi, Ijagboro Tracy, Ezema Joshua Tochukwu, Idahosa Miracle, Ifada Daniel, I extend my appreciation for your kindness and the friendship we shared and the collaborative spirit we fostered were instrumental in our collective growth, our shared challenges and successes forged lasting friendships, and I am grateful for the sense of community we cultivated during our academic journey together.

I want to emphasize that this project success would not have been possible without the contributions of each and every one of you. Your support, guidance and belief in me have not only enriched this project but have also been instrumental in my personal and academic growth, thank you from the bottom of my heart for being an essential part of this journey.

TABLE OF CONTENT

ABSTRACT

This study examined the correlates of cybercrime and academic performance among secondary school students in Ikpoba Okha local Government Area, Benin City, Edo State. A sample of 100 copies of questionnaire was distributed randomly to 90 respondents in selected secondary school namely Ever Precious Group of school, Medna Group of school, Gloria Group of school at Ikpoba Okha. Based on the findings, it was revealed that students/ have knowledge of cybercrime and other internet related issues; that accessibility of technology is one of the major factors responsible for student involvement in cybercrime; that poverty and unemployment (as regards their caregivers or significant others) is responsible for involvement in cybercrime and that peer influence and frustration are active factors that lead to cybercrime. Secondary schools should come up with mechanisms for raising cybercrime awareness among the students. It can do so by organizing conferences and seminars and inviting cyber-security experts to give talks on the matters pertaining cybercrime. Secondary schools can also invite legal experts to inform students on matters pertaining cybercrime laws and cybercrime reporting. In addition, the secondary schools can raise awareness by creating a common unit for all the students in order to teach them about cybercrime. Such unit can include things like causes of cybercrime, effects of cybercrime and cybercrime laws. Government should adequately equip the Police force, Economic and Financial Crimes Commission (EFCC), Independent Corruption Practices Commission (ICPC) and other security operatives with improved technology to detect and prevent cybercrimes. Nigerian Government should enact stringent laws against cybercrime and ensure that violators are punished accordingly without discrimination.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE PROBLEM

The expansion of the internet and wider availability of computer technology have opened up new employment and economic prospects as well as chances for individuals who engage in unlawful activity. Not only has the prevalence of criminal activity increased dramatically as a result of technology and online communication, but it also seems to have given rise to a new sort of criminal activity. Legal systems and law enforcement are challenged by the increase in criminal activity and the possible introduction of new sorts of criminal conduct (Dennis, 2009). Cybercrime, according to Singh, Gupta, and Kumar (2016), is any illicit conduct that makes use of a computer as a tool, a target, or both. The term "cybercrime" has been used to describe a variety of offenses, including offenses against computer data and systems like hacking, offenses involving computer-related forgery and fraud like phishing, offenses involving content like disseminating child pornography, and copyright offenses like disseminating pirated content (Okanlawon, Yusuf, & Abanikannda, 2015). Any conduct utilizing computers and networks is considered a cybercrime. Cybercrime is a crime that is committed or enabled online. Any illegal behavior involving computers and networks is considered a cybercrime. This includes unsolicited emails and fraud (spam).It can include the distant theft of government or

corporate secrets through criminal trespass into remote systems around the globe. Cybercrime is not only limited to, anything from downloading illegal music files to stealing millions of dollars from online bank accounts, but also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the internet (Boniface & Michael, 2014).

Cybercrime is one of the world's fastest growing epidemic, and as technology progresses, so does the incidence of Cybercrime. Because of the ever-increasing rate of technological and information technology related improvements, the world would have been a better place with more chances. However, Cyber-related Crimes are also on the rise, with far-reaching consequences for the community at large. Students at practically all academic levels are active in Cyber Crime in some form (Agasi, 2010). Cybercrime is currently pervasive in Nigerian culture, with fraud being the most common type. This is due to the high prevalence of unemployment and other societal variables that keep the adolescents craving for more, particularly those who crave for material excess. Agasi, (2010) noticed that this encourages the youth to explore their talents in the online realm and how they might gain from it without being caught, knowing that Nigeria lacks adequate enforcement tools. Cybercriminals, who go by titles like "yahoo-yahoo," occupy a sizable portion of social media and the online ecosystem where money, data, and transactions are transferred. They live a luxury lifestyle and have a notorious persona thanks to the revenues of internet surfing. They even go so far as to combine spiritual aspects with internet browsing to cast a

spell on their victim, causing them to fall for their demand. All these impacts on university undergraduates and their academic achievement. Madume, (2012) observed that to the University students, the internet has the potential to affect education and national development, and this has inspired individuals, institutions, and organizations to construct cyber cafés where people may easily access knowledge from the internet. Opportunities of this kind are bound in Nigerian universities and other high institutions in accordance with the goals of tertiary education, which include, among other things, acquiring both physical and intellectual skills that will enable individuals to be self-reliant and useful members of society. Youths and most especially undergraduates account for a higher proportion of internet users, and there is a contradicting report on ICT competences and usage by gender, with males outnumbering girls. However, some people abuse these talents and misuse knowledge and information diversity, leading to illegality or cybercrime (Madume, 2012). The contribution of the internet to the academic development of among Nigerian undergraduate has been marred by the conscious evolution of new waves of crime. The internet has also become an environment where the most productive and safest offence thrives. Mutahir, (2019) expressed that cyber-crime has come as a surprise and a strange appearance that now lives with us in Nigeria. Because cybercrime is becoming an urgent and serious problem, one can expect that the number of cybercrime victims will increase in the future. Therefore, it is

important to gain the knowledge about the different factors that can lead to an increased or decreased likelihood of becoming a cybercrime victim.

The 1990s witnessed the rise of hacking culture, with various individuals exploring and testing the vulnerabilities of computer systems. While some hackers were motivated by curiosity and a desire to learn about technology, others engaged in malicious activities, leading to significant security concerns.

Governments worldwide recognized the need to address cybercrime. The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, was adopted in 2001 as the first international treaty that sought to harmonize national laws to combat cybercrime.

Over time, cybercriminals diversified their methods, leading to various types of cybercrime, such as phishing, malware attacks, identity theft, cyber stalking, and cyberbullying. Each new advancement in technology presented new opportunities for criminal activities. Growth of the internet and e-commerce: The increasing use of the internet for financial transactions and e-commerce led to a surge in online fraud and scams. Cybercriminals exploited weaknesses in online payment systems.

For the past several decades, the introduction of information and communications technologies [ICT] has resulted in tremendous improvements in many areas of human endeavors. It is seen as a crucial aspect of globalization, which connects the

world with a wide range of assets [Igie, 2015]. The internet provides students with numerous benefits, including simple access to knowledge and the ability to link to the rest of the world. These help they develop cognitively |and socially [Johnson, 2010]. Since the beginning of the internet and electronic revolution in Nigeria, the level of cybercrime has risen dramatically. In just over two decades, the internet has expanded in such proportions it becomes an integral part of the lives of thousands of people all over the world [Warner, 2011]. Students will benefit greatly from having access to the efficient web capacity in schools since it will enhance their level of understanding, writing abilities, and academic achievements by allowing them to browse the internet. However, if this is done unmanaged, it may lead to cyber-criminality among students [Singh and Bala, 2014].

Singh and Bala [2014] posited that young students having unrestrained and persistent use of the internet has the potential to reduce their productivity in class. It may lead them to becoming hackers and takes valuable time that could have been spent studying for higher grades.

Vast majority of students in Nigeria schools [secondary schools], have good comprehension and knowledge of cybercrime. youngsters as we have them today are also more acquainted with the four primary types of cybercrime which are; malware, financial fraud, illegal access, and cyber identity theft [Barfi, Nyagorme and Yeboah, 2018].

According to [Magele, 2011] The internet is becoming such a necessary evil that it has become a two-edged sword, creating benefits for people and organizations while also increasing the risk of data security. Without a question, the web has transformed and simplified everything in our lives including school, commerce, politics, and health. It has however brought with it certain elements of risks which we recognize as cybercrime. Over the last twenty years, cybercrime has emerged as a significant topic for investigators to study and investigate, as well as a growing issue for civil and public policy. Cybercrime is a term that covers all crimes conducted using computers, systems, phones, as well as crimes that do not rely primarily on technology [Britz,2015].

Cybercrime often called in Nigeria as ‘’YAHOO’’ through the web, is very frequent among Nigerian school aged children[secondary school students]. Nigeria today is not anything like the late 1990s, when only a few members of the minority rich classes had access to computers. The rise of E-waste has made it easier and inexpensive for most young people to purchase and own a used laptop at a low cost.

Some common types of cybercrime include:

Hacking: Unauthorized access to computer systems or networks to gain sensitive information or control over the target system.

Malware: The distribution and use of malicious software (malware) like viruses, worms, ransomware, and spyware to compromise systems, steal data, or disrupt operations.

Identity theft: Stealing personal information, such as social security numbers or financial details, to commit fraud or other crimes.

Cyberstalking and harassment: Using electronic means to repeatedly harass, threaten, or intimidate an individual or group.

Cyberextortion: Demanding money or valuable goods/services from an individual or organization under the threat of a cyber attack or damage.

Online fraud: Engaging in fraudulent activities, such as online auction fraud, investment scams, or fake online marketplaces.

As technology evolves, new forms of cybercrime continue to emerge, making it a significant challenge for law enforcement and cybersecurity professionals to combat these threats effectively. Preventing cybercrime involves implementing robust security measures, raising awareness about potential risks, and adhering to best practices to protect sensitive information online.

1.2 STATEMENT OF THE PROBLEM:

Recently, most crimes have shifted from the streets to electronic platforms on the internet, with the internet's contribution to academic progress among Nigerian secondary school students tainted to the deliberate emergence of fresh waves of criminality refer to cybercrime. The internet has also become a breeding ground for the most prolific and risk-free offense. Cybercrime has come as a surprise and a weird presence in Nigeria for the time being. With each passing day, we witness an increase in the number of worrisome incidents of cybercrime perpetrated by Nigerian secondary school students, with each new happening more distressing than the one before. It has become a tenacious mouth sore that gives us a lot of agony and embarrassment because criminally minded secondary school students are stealing and committing all sorts of academic and economic crimes with the use of online communication and transactions on the internet. In most cases, various forms of crimes are being witnessed ranging from exam negligence's, falsification of admission, rape, robbery and stealing, sexual molestation, onslaught, cultism and drug abuse. With this current happening, the face of the Nigerian institution at large has suffered a lot of setbacks. It is against this backdrop it has become necessary to examine the correlates of cybercrime and academic performance among secondary school students.

1.3 OBJECTIVE OF THE STUDY:

The main objective of the study is to evaluate the impact of cybercrime on the educational performance of selected secondary school namely Ever Precious Group of school, Medna Group of school, Gloria Group in Ipoba Okha local Government Area and to proffer possible panacea.

SEEKS TO:

i. determine the perception of secondary school students toward cybercrime in Ikpoba Okha local government area
ii. examine the influence of cybercrime on the educational performance of secondary school students.
iii. outline the various forms of cybercrime carried out by secondary school students.
iv. examine the negative impacts that cybercrime poses to the student and society

1.4 RESEARCH QUESTIONS

The research will be guided by the following research questions.

i. what is the perception of secondary school students towards cybercrime

ii. what influence cybercrime has on the educational performance of secondary school students

iii. what are the various forms of cybercrime carried out by secondary school students

iv. what are the negative impact cybercrime poses to the student and society at large.

1.5 SIGNIFICANCE OF THE STUDY

The study will give insights to what cybercrime is and its impact on the academic performance of secondary school students inikpoba okha local government area.The study will explore various types of cybercrime, and the information generated through the study will be useful to know in what way it has impacted to the lives of students and also ways with which to curb it from among students and society at large in Nigeria. Findings from the study will be helpful to government, management of academic institution and security agencies. It will provide the government with framework of information regarding the need for them to strengthen its security agencies which is saddled with the arduous responsibility of fighting cyber crimes in Nigeria. To security agencies, the study will enlighten them on the need to sustain

the ongoing aggressive onslaught on cyber criminals in Nigeria. To institution of learning, findings from the study will reveal the need to include studies on cyber crime to enlighten student on the negative effect of engaging in it. Empirically, the study will contribute to the general body of knowledge and serve as a reference material to both scholars and student who wishes to conduct further studies in related field.

The study has significance to promote social work practice by identifying interventions at macro, mezzo, and micro levels. The research also fills the identified literature gaps. Over all, it suggests possible recommendations for policy and framework gaps in rehabilitation and reintegration of secondary school students. This helps stakeholders to be proactive in planning future intervention programs thereby enhancing the probability of success in curbing cybercrime.

1.6 SCOPE OF THE STUDY

This study will focus on critically analyzing the correlates of cybercrime and academic performance among secondary school students in ikpoba okha local government area.

1.7 DEFINITION OF TERMS

Cybercrime is any criminal activity that involves a computer, networked device or a network.

Information communication technology is defined as a diverse set of technological tools and resources used to transmit, store, create, share or exchange information.

Cyber security Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes

Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data

Cyber space Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication.

CHARTER TWO

LITERATURE REVIEW

This chapter is concerned with the review of relevant literature on the correlates of cybercrime and academic performance among secondary school students. There have been constant issues surrounding cybercrime and academic performance among students. A number of studies and theories have provided reviews, some of which are examined in this study.

2.1 CYBERCRIME: GLOBAL PERSPECTIVE

The fraudsters normally depict themselves to be personalities they are not and tries to convince victims to believe that they are actually the people they are pretending to be. The internet has given the chance to people to commit different kinds of offenses and atrocities everywhere across the globe. Reasentse (2015) stated that cyber harm is a worldwide worrisome development for all nations both locally and globally. Studies have shown that 64% and 58% of guys and ladies respectively are mostly probable to become victims of cybercrime. Similarly, Reasentse (2015) reported that the majority of cybercrime victims are located in Russia (85%), China (77%) and South Africa (73%). Reasenntse (2015) articulated that 67% and 17% came from the United Kingdom and the United States of America respectively, 12% and 4% were from Australia and other nations, respectively. The survey further acknowledged different forms of cyberbullying found various social networks, indicating that; 7 out of 10 young people have been victims of cyber-bullying, and 37% have experienced cyber-bullying on a highly frequent basis and 20% have experienced extreme cyber-bullying on a daily basis. The results again indicated that the most common social networks for cyberbullying were Facebook (54%), Twitter (28%) and Ask FM (26%). Internet Crime Complaint Center (IC3, 2008) internet crime report indicated that around two hundred seventy-five thousand two hundred eighty-four (275, 284) individuals lodge complaints of a total loss of US$265 million in the United States alone, with victims on average losing about US$931. The report further stressed that

the crime rate have moved up by 33.1 percent from the previous year (IC3, 2008). According to Symantec Global Internet Security Threat (SGIST) Report (2018) e-mail spam has risen 54.6 to 55 percent from 2017 to 2018 globally. Saudi Arabia takes the lead of global spam rate with 66.8% followed by China 62.2% and Brazil 60%. The scammers launched their targeted spam on the areas of mining, finance, insurance and real estates, etc. In the reports, the results showed that; Mining representing 58.3%, Finance, Insurance & Real Estate all representing 56.7 % and Manufacturing with 55.1%. The report indicated that an average of 55 organizations both small-medium and small businesses was attacked in 2018 globally. Greater numbers of attacks are from hacking. Theft or loss of a computer are the most common results of data breaches which criminals normally relied heavily on intimidate victims.

2.2 CYBERCRIME: AFRICAN CONTINENT

The infiltration and acceptance of Information and Communication Technologies (ICTs) in African has taken the continent to a different level. Even though, accessibility and use of some internet amenities on some parts of Sub-Saharan Africa is still hook up to internet cafés to solve online problem. Countries like Nigeria, Cameroon and Ghana have well established modern internet facilities which are accessible via satellite connections and fiber optic cables. This upsurge in diffusion

of ICT has resulted ICT oriented businesses such as e-banking, e-governance, e-justice, telemedicine and many more, particularly in West African coast. However, this boost of ICT has bred a new level of criminal offences called cybercrime. The internet has described as a necessary evil providing chances for people and institutions and also carrying with it a serious threat to global internet cyber security (Boateng, Longe, Mbarika, Avevor, & Isabalija, 2010). A study by Akuta, Ong'oa, & Jones (2011) reported that although the African continent was considered as ―backwards, it has adopted the ICT world strongly. Internet World Stats acknowledged that the internet use in Africa continent had reached 2.3% of the total global use by December 2007. Africa‘s internet use between the periods of 2000 to 2007 had increased by 423.9% against 180.3% for the rest of the world (Akuta et al., 2011). In a continent that is characterised by high incidence of poverty and increasing youth unemployment governed corruption, the exhibition of money and flashy cars and wealth by cybercriminals can easily pull the unemployment poor young men to join the cybercrime fraternity. As a result a growing number of youth are resorting to cybercriminals in Africa. This white color crime has variety of names, it known in Nigeria as the „Nigerian letter‘or „419‟, ‗Sakawa‘or ‗Yahoo-yahoo‘in Ghana and „Faymania‘ in Cameroon (Atta-Asamoah, 2009). The increasing usage of the Internet in Africa continent made the Internet and other online means of communication very common. This has brought opportunities for the establishment of online businesses. This has also brought about similar new challenges of

cybercrime leading to mistrust among nations, companies and individuals across the world. The widespread nature of cybercrime in Africa has been a worrying issue for all. There is generally low safety and consciousness awareness training programmes from the security agencies available to educate people from becoming victims of cybercrime. These criminals often commit these crimes and go unpunished. This issue gets disturbing when studies revels that Sub Sahara Africa holds a record of four countries (Nigeria Cameroon, Ghana and South Africa) among the top ten countries globally engaged cybercrime (Reasentse, 2015). Nigeria is observed as the nucleus or safe haven for cybercrimes around the globe which has been earmarked by the international community for their allege envelopment in such a wicked cybercrime. The country has been graded 3 rd globally after the USA and Britain and number one in Sub Sahara Africa (Merwe, 2015). Cybercrime is the fastest growing area of criminality among crime. Day in day out criminals are abusing and manipulating the internet with anonymity to commit different kinds of crimes globally. These crimes come in various format which causes serious harm and threat to global peace and cyber security. Atta-Asamoah (2009) articulated that during the last two decades many uninvited e-mails and other related letters were spreading from the Africa. Such letters were so tempting and inviting and it normal contain fraudulent information such as business proposals, inheritance reclamation, job offers, announcement of lottery wins, marriage proposals, immigration offers, admission to overseas academic institutions to money transfers and property sales,

among others. Nigeria is the originator of such crimes. However, this practice has recently engulfed many youth in West Africa spending sleeping sleepless nights in cybercafé scouting for victims online to draw millions of dollars from innocent people across the globe. Boateng et al. (2010) found that majority of agents of cyber criminals are teenagers under school going ages of 15 years in Ghana. They form 88% representing the bulk of the respondents. This was affirmed by the Commercial Crime unit of the Ghana Police Service in an interview. They declared that majority of cybercriminals are adolescents representing 85%. Related crimes comprise child pornography, hacking sites to get access to credit cards and downloading films for sale

2.3 CYBERCRIME IN NIGERIA

If there is any lesson from the Covid-19 pandemic across the world, it is in how Information and Communications Technology (ICT) systems are now as basic to our lives as water and electricity. During the lockdown that lasted several months in many countries, it was technology that enabled people and businesses to be connected. Today, many individuals, corporate organizations and government agencies depend on ICT and computer networks to perform simple as well as complex tasks – from social networking and research to business and commerce. But cyberspace is vulnerable to the antics of criminals, especially in Nigeria where internet scams are reported to have increased by more than 50 per cent in the past

two years. Cybercrimes, as most people are already aware, refer to criminal acts such as identity theft and bank frauds facilitated using the internet. Sadly, to our collective shame, Nigeria is often cited as a breeding ground for most of these nefarious practices because of the activities of some of our citizens. In recent years, many criminal elements have been using these modern telecommunication networks to commit all manner of crimes that give us a bad image globally. Last month in the United States, a Nigerian social media influencer, Ramon Abbas, aka 'Hushpuppi' was sentenced in Los Angeles to more than 11 years in prison. Abbas, 40, was also ordered to pay $1.7m in restitution to two fraud victims, according to a statement from the United States Department of Justice. Abbas, according to the American prosecutor, laundered money from various online crimes including business email compromise, a crime in which criminals hack into email accounts, pretend to be someone they're not, and fool victims into wiring money to them.

Indeed, there is an upsurge of cybercrime in Nigeria. The country is ranked third in global internet crime while 7.5 per cent of the world's hackers are said to be Nigerians. Committed mostly by the young, often called "Yahoo" boys, a precursor of the infamous '419' email scammers, the fraudsters are increasingly taking advantage of the rise in online transactions, electronic shopping, e-commerce, and the electronic messaging systems to engage in all manner of crimes. The Central Bank of Nigeria (CBN) has consistently reported that about 70 per cent of attempted

or successful fraud/forgery cases in the Nigerian banking system were perpetrated via the electronic channels. This is a disincentive for foreign investment.

In 2015, the Cybercrimes Act was passed into law to address the challenges. The law criminalizes a variety of offences – from ATM card skimming and identity theft to possession of child pornography. It imposes, for instance, seven years imprisonment for offenders of all kinds and additional seven years for online crimes that result in physical harm, and life imprisonment for those that lead to death. But like almost every law in the country, there is the problem of enforcement. The "yahoo boys" still daily throng cybercafé premises to "transact" their business with the owners looking away. Yet the law criminalizes internet café owners who knowingly allow their premises to be used to commit crimes.

Cybercrime has evolved over the past years from the [419] we know it to be called over a decade ago to more subtle form which is currently recognized in Nigeria as [yahoo boys].

2.4 CAUSES OF CYBERCRIME AMONG SECONDARY SCHOOL STUDENT

1**. Poverty**: This i would say is one of the major causes of students engaging themselves in cybercrime as they often come from poor background or family, facing the economic situation of the country such as the high cost of living, low

salary payments, lack of care and support to secondary school students by giving grants and scholarship to deserving students and are most probably denied basic necessities of live often result to cyber crime as a last resort.

2. **The Get Rich Quick Syndrome**

The get-rich-quick syndrome has been described as a major factor impeding economic development in Nigeria. A lecturer and professor of physics from Augustine University, Ilara-Epe (AUI), Prof. Abiola Ogunde, stated this while speaking as lecturer on "Get-Rich-Quick Syndrome," at the eighth matriculation of the institution recently.

According to him, the get-rich-quick syndrome was one of the contemporary social problems of Nigerian society and could be described as culture of quick fixes or shortcuts that is prevalent among youths, which is unlawful, unreasonable, untenable and even ungodly. He added that Nigerian youths were no longer interested in earning money through the legitimate and honourable way, which is one of the major reasons for present economic decline. Ogunde mentioned illegitimate acts like armed robbery, political thuggery, kidnapping, Internet fraud, ritual killings and others, adding that teenagers and university undergraduates who believe education is a scam are mostly found in these illegal acts.

In a society where materialism and unequal distribution of wealth is the order of the day, there is always an alarming rate of crime and social vices. Get-rich-quick syndrome is slowly killing Nigerians especially the youth. The quest for wealth and luxury have led to an increase in crime and disregard for law and order in society with the kidnapping and killings of people for money rituals increasing on a daily basis. In recent years, due to the economic backlash and the desire to 'belong' many youths have taken to kidnapping and killings.

Get-rich syndrome and the future of Nigerian youth

Many of our youths have dropped out of school while cybercrime is becoming common amongst them. Between late December 2021 and January 2022, footages of killings for rituals were seen daily on the social and mainstream media. In several cases, bodies were found with several parts missing. The reason for these atrocities is mostly attributed to unemployment and bad government but what about the uneducated who indulge in such acts?

It is more worrisome when a number of those found to be involved are teenagers, which raises an alarm on parenting. This may also be attributed to neglect of our educational system because if our youths are fully engaged in school activities, they may not find time to indulge in this. Unless this is stopped, the future of Nigerian youths will be jeopardised as crime will be the order of the day and there will be no regard for law and order which is essential for peace and development of society.

“This desperation by our youths to survive at all costs is dangerous, devastating and pathetic. It poses a serious threat to the Nigerian society, particularly the upcoming generation, if the trend is not urgently addressed,” Ogunde said.

3. **Peer Pressure:**

The study showed that a lack of self-control is also a major predictor of children's cybercrimes. Risk-taking, impulsive kids are more likely than other children to act on an opportunity to commit illegal online activities, said Thomas Holt, a Michigan State University criminologist who led the study.

"It's important to know what your kids are doing when they're online and who they are associating with both online and offline," Holt was quoted as saying by Live Science.

Cybercrimes include digital piracy, such as "stealing" music or movie files by downloading them without paying, or online bullying and harassment, which can consist of sending threatening or sexual messages via email or text message.

Computer hacking, also known as cyber-trespassing, and viewing online pornography, which is illegal for those under 18, are also cybercrimes.

It’s important to note that cyber security laws and regulations regarding data privacy and protection are continuously evolving, and many more state laws and regulations

regulate this area, depending on the state. It's recommended to check all the cyber security laws by state to ensure compliance.

Cybercrime has been on the agenda of the Nigerian Government for many years. Investigations – in particular of fraud-related cybercrime – have been carried out in particular by the Economic and Financial Crime Commission (EFCC).

Though the Evidence Act was amended in 2011 to cater for the admissibility of electronic evidence, the absence of a legal framework on cybercrime hampered effective criminal justice measures until 2015.

In February 2015, the Government adopted the National Cybersecurity Policy and Strategy prepared by the Inter-Ministerial Committee coordinated by the Office of the National Security Adviser. It is based on the understanding that threats to information and communication technology are threats to Nigeria national security touching the "economic, political and social fabric of Nigeria." The most significant threats identified are cybercrime, cyber-espionage, cyber conflict, cyber-terrorism and child online abuse & exploitation.

The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 was enacted and entered into force on 15th May 2015. The purpose of the Act is also to promote cybersecurity and cybercrime prevention, and it provides for obligations to the private sector – including ISPs, telecommunication operators and financial

institutions – to report and cooperate with law enforcement authorities and the Nigerian Computer Emergency Response Team (ng-CERT). It provides for the National Security Adviser to coordinate LEAs and the Attorney General to oversee and strengthen the legal and institutional framework whilst establishing a Cybercrime Advisory Council to facilitate effective implementation, capacity-building, multi-stakeholder engagement and inter-agency/international cooperation.

The Nigerian Computer Emergency Response Team was established in the Office of the National Security Adviser. Its mission is "To manage the risks of cyber threats in the Nigeria's cyberspace and effectively coordinate incident response and mitigation strategies to proactively prevent cyber-attacks against Nigeria". The core function of ngCERT are:

- To establish a shared Situation Awareness platform - Coordinate information sharing at the National Level
- To efficiently manage and coordinate management of incident of national interest
- To support the National Cybersecurity Policy
- To provide technical support and expertise to sectorial CSIRT's as and when required
- To serve as international Point of contact for all Internet Security Incident in Nigeria.

In March 2016 – in line with Articles 42 and 43 Cybercrimes Act – the Cybercrime Advisory Council is to be established, comprising representatives of a wide range of ministries and agencies under the overall coordination of the National Security Adviser. Functions include:

Creating an enabling environment for sharing of information and experience

Formulating policy guidelines regarding implementation of provisions of the Cybercrimes Act 2015

Advice on preventive and other measures regarding cybercrime and cybersecurity.

In 2019 the Data Protection Bill passed the approval of the National Assembly, but it wasn't signed by the President. Following the presidential elections though, the proposal had to go back to the approval of the Parliament and it is currently being revisited to restart the legislative process.

Nigeria: Cybercrimes And Cyber Laws In Nigeria: All You Need To Know

Nigerians have become cyber-creatures, spending a significant amount of time online. As the digital world expands, so does cybercrime in Nigeria. The necessity to combat these seemingly uncontrollable phenomena gave rise to Cyber Laws in Nigeria.

Cyber law acts as a shield over cyberspace, preventing cybercrime from occurring. The government is committed to developing and enforcing regulations to combat illicit online activities.

The "Cybercrimes (Prohibition and Prevention) Act, 2015" has a significant impact on cyber law in Nigeria. This Act creates a comprehensive legal, regulatory, and institutional framework in Nigeria to prohibit, prevent, detect, prosecute, and punish cybercrime.

The Act also encourages cybersecurity and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights, as well as the protection of important national information infrastructure.

What is a Cybercrime?

Cybercrime is a type of crime that takes place in cyberspace, or in the realm of computers and the Internet. Because our society is evolving towards an information society where communication occurs in cyberspace, cybercrime is now a global phenomenon. Cybercrime has the potential to significantly influence our lives, society, and economy.

What is Cyber Law?

Any law that deals with the internet and similar technology is known as cyber law. Cyber Law is frequently referred to as "Law of the Internet" or "IT Law." It's a legal framework for dealing with issues relating to the Internet, computing, Cyberspace, and other associated matters.

One of the newest aspects of the legal system is cyber law. This is due to the rapid advancement of internet technology. People who use the internet have legal safeguards under cyber law. This applies to both business and common citizens. Anyone who uses the internet should be familiar with cyber laws.

Intellectual property, contract, jurisdiction, data protection laws, privacy, and freedom of expression are all covered by cyber law. It oversees the distribution of software, information, online security, and e-commerce via the internet. E-documents are given legal validity in the field of Cyber Law. It also establishes a framework for e-commerce and e-filling.

To put it another way, Cyber law is a legal framework for dealing with cybercrime. Due to the increased use of E-commerce, it is critical that suitable regulatory practices are in place to ensure that no malpractices occur.

Cybersecurity laws vary a lot from country to country and jurisdiction to jurisdiction. Penalties depend on the nature of offence, and will range from a fine to

imprisonment. It is critical for citizens to understand their particular countries' cyber laws in order to ensure that they are fully informed about all cybersecurity issues.

Categories of Cybercrime in Nigeria:

Cybercrimes against People:

Cybercrimes against people include cyber harassment and stalking, e-mail phishing, the dissemination of child pornography, various sorts of spoofing, credit card fraud, human trafficking, identity theft, and online connected libel or slander.

One of the most serious Cybercrimes nowadays is the trafficking, distribution, publishing, and dissemination of obscene material, such as pornography and indecent exposure. The potential harm to humanity from such a crime cannot be overstated. If not managed, this is one cybercrime that threatens to impair the progress of the younger generation as well as leave irreparable scars and injuries.

Correspondingly, in Nigeria prior to the gruesome murder of Cynthia Osokogu in July 2012, as reported by an online news magazine, people had suffered a similar fate. For example, Uzondu, an undergraduate student at a private Christian university in Ogun State, allegedly contracted the dreaded Human Immune Virus, HIV, from a man she thought was her boyfriend.

The victim met the con man on the famous social networking platform, Facebook, and before she knew it, she was whisked away to a fantasy holiday where she was

lavished with expensive presents such as an iPad and the latest BlackBerry phone, among other things. During these amorous outings, the young girl became pregnant, but her partner was nowhere to be found. Unfortunately, she has no idea who the man was, no contact information, and no place of employment. Worse still, she tested positive for HIV.

Cybercrime against property

The second type of cybercrime is cybercrime against all types of property. Distributed Denial of Service (DDoS) attacks, hacking, virus transmission, cyber and typosquatting, computer vandalism, copyright infringement, and Intellectual Property Right (IPR) breaches are examples of these crimes.

Cybercrime against the Government:

The third category of cybercrime is cybercrime against the government. When a cybercrime is committed against the government, it is considered an attack on the sovereignty of a nation and an act of war. Hacking, gaining access to confidential information, cyber warfare, cyber terrorism, and the use of pirated software are all examples of cybercrime against the Government.

The expansion of the Internet has revealed that the channel of Cyberspace is being used by people and groups to threaten foreign governments as well as intimidate a

country's citizens. When an individual hacks into a government or military-run website, the offense becomes terrorism.

Most of these types of cybercrimes have been addressed by the Cybercrimes Act of 2015.

Cybercrimes (Prohibition and Prevention) Act, 2015

The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

Cybercrimes highlighted under this ACT include:

- Offences against critical national information infrastructure
- Hacking Computer Systems and Data Alteration
- Unauthorized Access of Protected Systems
- Illegal Registration of Cybercafé or Usage of Unregistered Cybercafé
- Computer related fraud
- Theft of Electronic Devices
- Unauthorised modification of computer systems, network data and system interference
- Publishing False Digital Signature and Certificates
- Cyber terrorism

- Exceptions to financial institutions posting and authorised options
- Fraudulent issuance of e-instructions
- Tampering with Computer Source Documents
- Identity theft and impersonation
- Child pornography and related offences
- Cyberstalking
- Cybersquatting
- Racist and xenophobic offences
- Attempt, conspiracy, aiding and abetting
- Importation and fabrication of e-tools
- Breach of Confidentiality and Privacy
- Manipulation of ATM/POS Terminals
- Phishing, spamming, spreading of computer virus
- Electronic cards related fraud
- Use of fraudulent device or attached e-mails and websites

2.4.1 Administration and Enforcement Cyber Law in Nigeria

Under the 2015 Cybercrime Act, the National Security Adviser's office serves as the coordinating body for the security and enforcement authorities. The Attorney-General of the Federation reinforces and improves Nigeria's existing legal frameworks regarding cybercrime.

All law enforcement, security, and intelligence agencies develop the institutional capacity necessary for the effective implementation of the provisions of the 2015 Cybercrime Act, and in collaboration with the Office of the National Security Adviser, initiate, develop, or organize training programs for officers charged with cybercrime on a national or international level.

2.4.2 Establishment of the Cybercrime Advisory Council

To Coordinate Cybercrime Act 2015, there was established a Cybercrime Advisory Council (in this Act referred to as "the Council") incharge of handling issues relating to the prevention and combating of cybercrimes, cyberthreat, computer-related cases and the promotion of cybersecurity in Nigeria.

The Cybercrime Advisory Council comprises of a representative each of the following Ministries, Departments and Agencies –

- Federal Ministry of Justice;
- Federal Ministry of Finance;
- Ministry of Foreign Affairs;
- Federal Ministry of Trade and Investment;
- Central Bank of Nigeria;
- Office of the National Security Adviser;
- Department of State Services;

- Nigeria Police Force;
- Economic and Financial Crimes Commission;
- Independent Corrupt Practices Commission;
- National Intelligence Agency;
- Nigeria Security and Civil Defence Corps;
- Defence intelligence Agency;
- Defence Headquarters;
- National Agency for the Prohibition of Traffic in Persons;
- Nigeria Customs Service;
- Nigeria Immigration Service;
- National Space Management Agency;
- Nigerian Information Technology Development Agency;
- Nigerian Communications Commission;
- Galaxy backbone;
- National Identity Management Commission;
- Nigeria Prisons Service;

What is the Importance of Cyber Laws in Nigeria?

Cyber law is important for organizations that are exposed to risk as a result of an inefficient cybersecurity system. These laws apply to all forms of corporate organizations and digital systems that do business on a daily basis. Each organization

adheres to unique cybersecurity guidelines, cybersecurity legislation, cybersecurity policies, and legal issues regulations

2.5 REHABILITATION AND REINTEGRATION

Our youths must understand that the legal means of wealth acquisition is through hard work, determination and dedication and resourcefulness. I urge the youth to embrace entrepreneurship and skills acquisition so as to be independent and avoid social malpractices.

Parents should give their wards adequate training so as to divert their minds from quick wealth syndrome. Also, parents should monitor the kind of friends their wards associate with.

The authorities and security agencies should work together to stop ritual killings in the country. This can be done with the rebuilding of the educational and industrial sector to address unemployment.

He said: “The society that ought to query the source of their wealth ends up celebrating them. We live in a time where a child can afford to buy houses or cars for parents without the moral stand of those parents to query the sources of the stupendous wealth.

2.5.1 Theoretical Framework

The father of CLASSICAL CRIMINOLOGY also known as CHOICE THEORY,CESARE BONESANA posited in his book (crimes and punishments) 1764. that individuals are rational human beings that pursue their own interests, which often leads them to harm one another. People commit crime because they "Choose" to do it. Individuals attempt to maximize their pleasure and minimize their pain.

ADAMS SMITH the father of RATIONAL CHOICE THEORY in his essay"An inquiry into the nature and causes of the wealth of nations" Holds that people are rational and weigh the potential costs and benefits of committing crime. The most common benefit and motive for hackers is "thrill-seeking." In order for punishments to be effective, they must be KNOWN, SWIFT, CERTAIN, and SEVERE.

Social Control Theory

Hirschi (1969) explains, the Social Control Theory proposes that exploiting the process of socialization and social learning builds self-control and reduces the inclination to indulge in behavior recognized as antisocial. This theory emphasizes on the role of society in the control of criminal behavior. It specifies the fact that no society can afford to denounce criminal activity without duly accepting its

responsibility towards the same. Theory of Social Control stresses on the fact that most delinquent behavior is the result of unmonitored 'Social Control' by the authorities and primarily, the family. The theory is indicative of the fact that relationships and commitments with respect to set norms and a belief structure encourage or discourage individuals and groups to break the law.

CHAPTER THREE

METHODOLOGY

Methodology is a very important and powerful tool in research undertakings. It is a key to proper conduct and understanding of a research work. Research methodology seeks to put into proper prospective the topic under study. The oxford advanced learners dictionary defines research as a careful study of a subject, especially in other to discover new facts or information about it .This chapter covers the target population sample size, data requirements, method of data collection, method of data analysis, research instrument and actual field work.

3.1 STUDY DESIGN

Research design basically is a conceptualization of the methodology, it is concerned with the techniques used in the gathering of data for the research work (Izedonmi, 2008). It encompasses the sources of data collections, the population of the study, the sample size as well as the data analysis techniques.

For the purpose of the study, the cross sectional survey research design was adopted in this study because the data was collected at a particular time. This is the specification of the methods and procedures for acquiring the information needed for the research.it involved conducting interviews and circulation of carefully designed questionnaires to the selected secondary school students namely Ever Precious

Group of school, Medna Group of school, Gloria Group in Ikpoba Okha local Government Area of Edo State.

3.2 SCOPE OF STUDY

The study aims to explore the causation between cybercrime and academic performance by examining the factors that contribute to cybercrime activities such as anonymity, lack of parental control, weak internet security systems, and limited law enforcement. It also explores the strategies that schools and parents can use to mitigate the effects of cybercrime on students, such as policy implementation, awareness campaigns, parental control measures, and counseling services. The study focuses on secondary school students aged between 12-18 years old and takes place in selected secondary schools in a designated geographical location. The methods used in the study may include a questionnaire, interviews, and focus groups. The collected data analyzed using statistical software and presented in tables, graphs, and charts. Overall, this study aims to contribute to the understanding of the impact of cybercrime on secondary school students, increase awareness, and provide information for policy development aimed towards mitigating the impact of cybercrime.

3.3 POPULATION OF STUDY

population according to Agbonifoh and Yomere (1997) is the totality about whom the researcher wants to investigate. The population for this study is the two hundred and forty six(246) secondary school students in Ikpoba okha local government area from which a sample size was drawn.

3.4 SAMPLE SIZE AND SAMPLING TECHNIQUE:

A sample is a subject of the units of population in a portion or part of the subset of the units of the population of interest. Yaro Yamani sample selection method adopted in this study is stated below:

According to Yaro Yamani. $n=N/[1+(Ne^2)]$

Where: n is the sample size

N is the population,

e is the error limit (0.05 on the basis of 95% confidence level)

therefore: $n = 246/[1+246\ (0.05^2)]$

$n = 246/1.5625$

$n = 152$

3.5 INSTRUMENT OF DATA COLLECTION

The major instrument that was used for data collection during the research were questionnaires. Questionnaires are set of fixed pre-arranged and carefully typed questions which respondents provided answers to. It could also be said to be a document containing a set of questions designed in such a way that the research objectives were reflected in the questions for soliciting information from respondents on the subject of the research investigation.

3.6 METHOD OF DATA COLLECTION

In order for this study to come with a well articulated result, data was sourced from both primary and secondary sources. The essence is to serve as a guide as well as to gain a better and wider insight on the topic in order to give a fair judgment of the findings.

The primary sources are;

1) Questionnaire

The secondary sources are;

Literature text, periodicals such as journals, new dailies, seminar and conferences and unpublished write-ups.

3.7 METHOD OF DATA ANALYSIS

Data analysis is the breaking down and ordering of data into meaningful groups and search for pattern of relationship among these group. For the purpose of this study, chi-square (x^2) test will be used. This is because the chi- square (x^2) test is a method of comparing counted data or data measured in a normal scale in which individual observations are assigned to categories.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION

4.1 INTRODUCTION

The study made use of Likert-type question to gather information. The major aims and objectives of this research study was to evaluate and assess the impact of cybercrime on the education performance of secondary school students in Benin City, Edo State using Ikpoba Okha as a case study and to present information that will help investigate cybercrime in Nigeria. The research question was designed to capture the demographic data of the respondents and their opinions as regards the research question/statement, the questionnaire was divided into two (2) parts.

Part I sought to obtain information on demographic details of the respondent

Part II consisted of items measuring the respondents perceptions.

In all a total of hundred (100) questionnaires were administered to secondary school students in the study and ninety (90) were retrieved, one (1) was wrongly filled and nine (9) were not returned. Their responses are present in the tables below which was used to illustrate the responses received.

Number of responses

4.2 DATA PRESENTATION

Table 4.2.1: Demographic Details of Respondents

S/N	DETAILS	RESPONDENTS	FREQUENCY	PERCENTAGE
1	AGE	9-11	19	21.1
		12-14	31	34.4
		15-17	22	24.5
		18 and above	18	20
2	SEX	MALE	63	70
		FEMALE	27	30
3	CLASS	JSS1-2	40	44.5
		JSS3-SSS1	20	22.2
		SSS2	18	20
		SSS3	12	13.3
4	ETHINICITY	BENIN	68	75.6
		URHOBO	4	4.4
		IGBO	15	16.7
		YORUBA	3	3.3

Source: Field Survey,2023

Demographic data analysis: out of the one hundred copies of the questionnaires administered, a total of ninety copies were returned. Hence ninety usable copies of questionnaires were used for analysis. This represents an overall response rate of ninety percent ( ) for all respondents. These responses were used in providing answers to the questions raised in the study.

Table 4.2.1shows the breakdown of respondents sex. sixty-three male respondents representing seventy percent (70%) and twenty-seven female respondents representing thirty percent (30%) were surveyed in this study. This shows that the views of the respondents were sought across two sexes.

The study also made effort to analyze response from respondent perception and opinion on the various questions/statement raised in the part II section of the questionnaire.

Research question one: what is the perception of secondary school students towards cybercrime

Table 1: I feel well informed about cybercrime and its risk

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly Agree	60	66.7
Agree	19	21.1
Undecided	-	-
Disagree	11	12.2
Strongly Disagree	-	-
Total	90	100

Source: Field Survey,2023

Table 1: In the question,66.7% of the respondents hold a strong opinion that they are aware of cybercrime. While 21.1% merely agree. On the other hand 12.2% of the respondents disagree with the assertion from the table therefore, we can conclude that most respondents are aware of cybercrime.

Table 2: my school provides sufficient education about cybercrime

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Yes	67	74.4
No	11	12.2
Undecided	12	13.3
TOTAL	90	100

Source: Field Survey,2023

Table 2 as to the question from the table above, 67 which represents 74.4% said yes that they have had their account stolen or hacked. While 12.2% said no they have not experienced such on the other hand 12 respondents representing 13.3 remained undecided as regards the question asked. Therefore we can conclude that most respondents have been a direct victim of cybercrime

Table 3 I am cautious about sharing personal information online

RESPONDENTS	FREQUENCY	PERCENTAGE
Very often	27	30
Often	26	28.9
Not often	13	14.4
Not at all	24	26.7
TOTAL	90	100

Source: Field Survey,2023

Table 3 as regards the question, 30% of the respondents use very often while 28.9% often use the internet for educational purpose on the other hand 14.4% responded not often while 26.7 asserted not at all.

Table 4: I think cybercrime has serious consequences for the victim

RESPONDENTS	FREQUENCY	PERCENTAGE
Strongly agree	29	32.2
Agree	18	20
Undecided	10	11.1
Disagree	20	22.2
Strongly disagree	13	14.4
TOTAL	90	100

Source: Field Survey,2023

Table 4 in the question 32.2% of respondents held a strong view that cybercrime affects the educational performance of secondary school students .while merely 20% agree to the assertion. On the other hand 14.4% strongly disagree from the table below we can conclude that cybercrime affects the educational performance of secondary school students

Research question two: what influence cybercrime has on the educational performance of secondary school students.

Table 5: Cyberbullying and online harassment negatively affects my concentration and focus on school work

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
YES	78	86.7
NO	12	13.3
TOTAL	90	100

Source: Field Survey,2023

Table 6: I believe that exposure to cybercrime incidents has made me more cautious about my online activities and this has positively impacted my academic performance.

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly agree	46	51.0%
Agree	18	21.0%
Undecided	11	12.0%
Disagree	7	7.0%
Strongly disagree	8	9.0%
TOTAL	90	100%

Source: Field Survey,2023

Table6: above revealed that 21.0% of the total respondents were agree; 7.0% of the total respondents were disagree; 51.0% of the total respondents were strongly agree; 9.0% of the total respondent were strongly disagree; and 12.0% of the total respondent were undecided. This implies that the majority of the respondents were strongly agree.

Table 7: Cybercrime incidents such as hacking, identity theft have caused me stress and anxiety that has affected my school work.

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly agree	53	59.0%
Agree	13	15.0%
Undecided	10	11.0%
Disagree	6	7.0%
Strongly disagree	8	9.0%
TOTAL	90	100%

Source: Field Survey, 2023

Table7 above, it revealed that 15.0% of the total respondents were agree; 7.0% of the total respondents were disagree; 59.0% of the total respondents were strongly agree; 8.0% of the total respondent were strongly disagree; and 11.0% of the total respondent were undecided. This implies that the majority of the respondents were strongly agree.

Table 8: I believe that reporting cybercrime incidents to school authorities can help create a safer online environment for students

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly agree	43	48.0%
Agree	19	21.0%
Undecided	9	10.0%
Disagree	10	12.0%
Strongly disagree	9	9.0%
TOTAL	90	100%

Source: Field Survey, 2023

Table8 above, it revealed that 21.0% of the total respondents were agree; 12.0% of the total respondents were disagree; 48.0% of the total respondents were strongly agree; 9.0% of the total respondent were strongly disagree; and 10.0% of the total respondent were undecided. This implies that the majority of the respondents were strongly agree.

Research question three: what are the various forms of cybercrime carried out by secondary school students

Table 9:Have you ever engaged in cyberbullying

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly agree	43	51.0%
Agree	0	0%
Undecided	29	39.0%
Disagree	2	2.0%
Strongly disagree	8	8.0%
TOTAL	90	100%

Source: Field Survey, 2023

Table9 above, it revealed that 55.0% of the total respondents were agree; 34.0% of the total respondents were disagree; 6.0% of the total respondents were strongly agree; 0% of the total respondent were strongly disagree; and 5.0% of the total respondent were undecided. This implies that the majority of the respondents were agreed.

Table10: Have you ever hacked or gained unauthorized access to someone's online account

RESPONDENTS	FREQUENCY	PERCENTAGE
Strongly agree	21	24.0%
Agree	0	0%
Undecided	53	55.0%
Disagree	6	6.0%
Strongly disagree	15	15.0%
TOTAL	90	100.0%

Source: Field Survey, 2023

Table10 above, it revealed that 24.0% of the total respondents were agree; 0% of the total respondents were disagree; 55.0% of the total respondents were strongly agree; 6.0% of the total respondent were strongly disagree; and 15.0% of the total respondent were undecided. This implies that the majority of the respondents were strongly agree.

Table11: Have you ever engaged in online stalking or harassment

RESPONDENTS	FREQUENCY	PERCENTAGE
Strongly agree	37	41.0%
Agree	24	27.0%

Undecided	10	11.0%
Disagree	8	9.0%
Strongly disagree	11	12.0%
TOTAL	90	100.0%

Source: Field Survey, 2023

Table11 above, it revealed that 41.0% of the total respondents were agree; 27.0% of the total respondents were disagree; 11.0% of the total respondents were strongly agree; 9.0% of the total respondent were strongly disagree; and 12.0% of the total respondent were undecided. This implies that the majority of the respondents were agree.

Table12: Have you ever been tempted to respond to phishing scams

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly agree	13	15.0%
Agree	7	7.0%
Undecided	54	59.0%
Disagree	8	8.0%
Strongly disagree	10	11.0%

TOTAL	90	100.0%

Source: Field Survey, 2023

Table12 above, it revealed that 15.0% of the total respondents were agree; 7.0% of the total respondents were disagree; 59.0% of the total respondents were strongly agree; 8.0% of the total respondent were strongly disagree; and 11.0% of the total respondent were undecided. This implies that the majority of the respondents were strongly agree.

Research question four: what are the negative impact cybercrime poses to the student and society at large

Table13: cybercrime poses a significant threat to society

RESPONDENTS	FREQUENCY	PERCENTAGE
Strongly agree	21	24.0%
Agree	0	0%
Undecided	48	55.0%
Disagree	6	6.0%
Strongly disagree	15	15.0%

TOTAL	90	100.0%

Source: Field Survey, 2023

Table13 above, it revealed that 24.0% of the total respondents were agree; 0% of the total respondents were disagree; 55.0% of the total respondents were strongly agree; 6.0% of the total respondent were strongly disagree; and 15.0% of the total respondent were undecided. This implies that the majority of the respondents were strongly agree.

Table 14: cybercrime can lead to financial loses to individual and organisation

RESPONDENTS	FREQUENCY	PERCENTAGE
Strongly agree	45	51.0%
Agree	0	0%
Undecided	35	39.0%
Disagree	2	2.0%
Strongly disagree	8	8.0%
TOTAL	90	100.0%

Source: Field Survey, 2023

Table14 above, it revealed that 51.0% of the total respondents were agree; 0% of the total respondents were disagree; 39.0% of the total respondents were strongly agree; 2.0% of the total respondent were strongly disagree; and 8.0% of the total respondent were undecided. This implies that the majority of the respondents were agree.

Table15: Cybercrime has negatively affected my wellbeing

RESPONDENTS	**FREQUENCY**	**PERCENTAGE**
Strongly agree	18	21.0%
Agree	7	7.0%
Undecided	44	51.0%
Disagree	9	9.0%
Strongly disagree	12	12.0%
TOTAL	90	100.0

Source: Field Survey, 2023

Table15 above revealed that 21.0% of the total respondents were agree; 7.0% of the total respondents were disagree; 51.0% of the total respondents were strongly agree; 9.0% of the total respondent were strongly disagree; and 12.0% of the total

respondent were undecided. This implies that the majority of the respondents were strongly agree.

Table16: Cybercrime has affected my academic performance(e.g distraction and online cheating)

RESPONDENTS	FREQUENCY	PERCENTAGE
Strongly Agree	44	51.0%
Agree	7	7.0%
Undecided	18	21.0%
Disagree	12	12.0%
Strongly disagree	9	9.0%
TOTAL	90	100.0

Source: Field Survey, 2023

Table16 above revealed that 51.0% of the total respondents were agree; 7.0% of the total respondents were disagree; 21.0% of the total respondents were strongly agree; 12.0% of the total respondent were strongly disagree; and 9.0% of the total respondent were undecided. This implies that the majority of the respondents were agree.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 SUMMARY

In chapter one, an introduction to the study was given, highlighting the research question, objectives of the study and significance of the study. Chapter two presented a review of other relevant works that have been done on the subject while chapter three specifies the methodology adopted in conducting this research. Chapter four analyzed the results acquired from the research instrument (questionnaire).

5.2 CONCLUSION

This study examined the correlates of cybercrime and academic performance of students in selected secondary school namely Ever Precious Group of school, Medna Group of school, Gloria Group in Ikpoba Okha local Government Area, Benin City, Edo State. A sample of 100 copies of questionnaire was distributed randomly to 90 respondents in secondary schools at Ikpoba Okha. Based on the findings, it was revealed that students/ have knowledge of cybercrime and other internet related issues; that accessibility of technology is one of the major factors responsible for student involvement in cybercrime; that poverty and unemployment (as regards their caregivers or significant others) is responsible for involvement in cybercrime and that peer influence and frustration are active factors that lead to cybercrime. There is

much we can do to ensure a safe, secure and trust worth computing environment. As it is crucial not only to our general sense of wellbeing but also, to our national security and economy. The remarkable development in human history through computer technology has no doubt brought transformation in all aspects of life, especially in communication and information technology. Nevertheless, the internet has come with a lot of mixed feelings despite its numerous advantages to the secondary school students, and since people are valued regarding what they possess and command economically, the pressure to achieve success becomes intensified among the youths. This necessitated the ability of individuals to devise survival strategies and attain economic success by indulging in cybercrime. As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. In conclusion, cybercrime can significantly impact the educational performance of secondary school students by causing distractions, online bullying, loss of personal information, reduced internet access, and decreased trust in online platforms. To address these issues, a proactive approach involving education on online safety and responsible internet use, along with monitoring and support from schools and parents,

is essential to safeguard students' academic performance and overall well-being in the digital age.

5.3 RECOMMENDATIONS

In this regard, the following recommendations are suggested.

1. Seminars and workshops should be organized regularly to sensitize the public on the need to keep safe their personal information.

2. Secondary schools should come up with mechanisms for raising cybercrime awareness among the students. It can do so by organizing conferences and seminars and inviting cyber-security experts to give talks on the matters pertaining cybercrime.

3. Secondary schools can also invite legal experts to inform students on matters pertaining cybercrime laws and cybercrime reporting. In addition, the secondary schools can raise awareness by creating a common unit for all the students in order to teach them about cybercrime. Such unit can include things like causes of cybercrime, effects of cybercrime and cybercrime laws.

4. Authorities of Nigerian secondary schools should encourage and impact entrepreneurial skills on their secondary school students, whereby they can make money without getting involved in criminal activities.

5. Government should adequately equip the Police force, Economic and Financial Crimes Commission (EFCC), Independent Corruption Practices Commission (ICPC) and other security operatives with improved technology to detect and prevent cybercrimes.

6. Nigerian Government should enact stringent laws against cybercrime and ensure that violators are punished accordingly without discrimination.

7. Implement comprehensive cybersecurity education programs that teach students about online safety, responsible internet use, and the risks associated with cybercrimes.

8. Encourage parents to actively participate in their children's online activities by monitoring their internet use, discussing online safety, and setting reasonable screen time limits.

9. Develop and enforce clear anti-bullying policies in schools, including consequences for cyberbullying. Promote a culture of empathy and open communication.

10. Provide access to counselors or mental health professionals who can help students cope with the emotional and psychological effects of cyberbullying and other cybercrimes. Encourage students to participate in positive and educational online activities, such as research, collaborative projects, and skill development.

REFERENCES

Adams smith"*An Inquiry into the Nature and Causes of the Wealth of Nations*" in 1776.

Adeniran, A. I. (2008). *The Internet and Emergence of Yahoo-boys sub-Culture in Nigeria*. International Journal of Cyber Criminology, 2(2), 368–381.

Adesina, O. (2008). Secondary school students 'perceptions of incidences of internet crimes among school age children in Oyo and Ondo States, Nigeria (dissertation). University of Ibadan, Nigeria.

Akuta, E., Ong'oa, I. & Jones, C. (2011).'*Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law*, *Policy and Practice*,' Journal of Peace, Gender and Development Studies Vol 1(4) Pp129-137.

Atta-Asamoah, A. (2009). Understanding the West African cybercrime process. African Security Studies, 18(4), 105-114

Barfi, K.A., Nyagorme, P. & Yeboah, N. (2018). The Internet Users and Cybercrime in Ghana:Retrieved on 19th November 2022 from https://digitalcommons.unl.edu/libphilprac/1715/.

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. (2010). *Cybercrime and criminality in Ghana: Its forms and implications*. Paper presented at the Americas Conference on Information Systems.

Boniface, K. A., & Michael, K. A. (2014). *Curbing Cybercrime by Application of Internet Users' Identification System (IUIS) in Nigeria*. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 8(9), 1582-1585.

Britz, (2015)

Cesare Bonesana, Marchese di Beccaria. Dei Delitti e della Pene (On Crimes and Punishment) (1764):

Chawki, M. (2009). Nigeria tackles advance fee fraud. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/ jilt/2009_1/chawki/chawki.pdf

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.

Dominelli, "*Experience and Expression: Social and Cultural Significance in fear of Crime*,"The British Journal of Criminology, Volume 44, Issue 6, Pages 946–966, 1 November 2004.

Douglas, F., Kibet, N. & Panuel, P. (2022). *Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment*. International Journal of Cyber Criminology, 14(1), 283-299

Ewepu, G. (2016). Nigeria loses N127bn annually to cyber-crime. Retrieved Jun. 9, 2023 from https://bit.ly/2VaZns8

F. Agasi, F., (2010). *Gender, crime victimization, and fear of crime*," Security Journal, 22(1), 24-39

Hirschi's "social control theory (1969).

Igie, (2015)

Johnson, (2010)

K. Madume, R., (2012). *Women's fear of crime on university campuses: New directions*?" Security Journal, 22(1) 87-99,

Magele, T. (2005), E-security in South Africa, White Paper prepared for the ForgeAhead e-Security event 16/17 February 2006. [Online], Available at: www.forgeahead.co.za/ [Accessed 22 October 2009].

Makeri, Y. A. (2017). *Cyber Security Issues in Nigeria and Challenges.* International Journal of Advanced Research in Computer Science and Software Engineering. 2(2) 368-381,

Merwe, 2015

Moga, E., Salihu A., & Abdulkarim, R. (2019). *A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development.*" Journal of Research in Humanities and Social Science 9(9), 84-94.

Mutahir, W. E. (2019). *Cybercrime and the challenges of socio-economic development In Nigeria.* Journal of Research in National Development, 14(2).

Okanlawon, A. E., Abanikannda, M. O., & Yusuf, F. A. (2015). *University students' knowledge and attitude towards internet safety: a preliminary study*. Journal of Emerging Trends in Educational Research and Policy Studies, 6(3), 279-286. Retrieved on April 15, 2019 from https://bit.ly/2ve5QDY

Reasentse, T. (2015). Examining Media Portrayals of and Approaches to Cybercrimes in Botswana. Retrieved from: https://www.academia.edu/12944302/ on 10/2/2023

Ribadu, N. (2007). *Cyber-crime and commercial fraud: A Nigerian perspective.* Presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL (United Nations Commission On International Trade Law), Vienna, Austria, 9-12 July. Retrieved from http://www.cnudmi.org/ pdf/english/congress/Ribadu_Ibrahim.pdf

Singh and bola, (2014)

Singh, O., Gupta, P., & Kumarł, R. (2016). *A Review of Indian Approach towards Cybersecurity*. Retrieved on April 14, 2019 from https://bit.ly/2INZeEy

Warner, (2011)

QUESTIONNAIRE

DEPARTMENT OF SOCIAL WORK
FACULTY OF SOCIAL SCIENCES
UNIVERSITY OF BENIN,
BENIN CITY

Dear Respondents,

My name is **Nelson Ugwu,** I am an undergraduate student of the Department of Social work, University of Benin. I am carrying out an academic research on "the impact of single parenting on children upbringing and the implications of social work practice"**.** Participation on this study is on voluntary basis; therefore you are free to withdraw from the study at any time. I assure you that any information given will be kept confidential.

_____

Researcher

SECTION A: (demographic information)

Instruction: Please tick the most appropriate answer that is applicable to you

Sex: Male ( ) Female ( )

Religion: Christianity ( ) Islam ( ) Traditional African Religion ( )

Age: 9-11 ( ) 12-14 ( ) 15-17 ( ) 18 and above ( )

Class: JSS1-2 ( ) JSS3-SS1 ( ) SSS2-3 ( )

SECTION B: Research Question

Instructions: Please tick the appropriate column, one that best represent your opinion in each of the following statements.

Key: A – Agree, SA – Strongly Agree, U – Undecided and D – Disagree and SD – Strongly Disagree

S/N	Item	SA	A	D	SD
	what is the perception of secondary school students towards cybercrime				
1	I feel well informed about cybercrime and its risk				
2	my school provides sufficient education about cybercrime				
3	I am cautious about sharing personal information online				
4	I think cybercrime has serious consequences for the victim				
	Research question two: what influence cybercrime has on the educational performance of secondary school students.				
5	cyberbullying and online harassment negatively affects my concentration and focus on school work				
6	I believe that exposure to cybercrime incidents has made me more cautious about my online activities and this has positively impacted my academic performance				
7	cybercrime incidents such as hacking, identity theft have caused me stress and anxiety that has affected my school work.				
8	I believe that reporting cybercrime incidents to school authorities can help create a safer online environment for students				
	Research question three: what are the various forms of cybercrime carried out by secondary school students				

9	have you ever engaged in cyberbullying				
10	have you ever hacked or gained unauthorized access to someone's online account				
11	have you ever engaged in online stalking or harassment				
12	have you ever been tempted to respond to phishing scams				
	Research question four: what are the negative impact cybercrime poses to the student and society at large				
13	cybercrime poses a significant threat to society				
14	cybercrime can lead to financial loses to individual and organization				
15	cybercrime has negatively affected my wellbeing				
16	cybercrime has affected my academic performance(e.g distraction and online cheating)				