THE IMPACT OF CYBERCRIME IN BENIN METROPOLIS

BY

EJOHWOMU FREEBORN AKPEVBOGHENE

PSC1611548

DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF PHYSICAL SCIENCE

UNIVERSITY OF BENIN

BENIN CITY

IMPACT OF CYBERCRIME IN BENIN METROPOLIS

BY

EJOHWWOMU FREEBORN AKPEVBOGHENE

PSC1611548

BEING A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, IN PARTIAL FULFILEMENT OF THE FOR THE AWARD OF THE BACHELOR OF SCIENCE (B.S.C) DEGREE IN COMPUTER SCIENCE, FACULTY OF PHYSICAL SCIENCE, UNIVERSITY OF BENIN

NOVEMBER 2022.

CERTIFICATION

This is to certify that this project work was carried out by EJOUWOMU FREEBORN AKPEVBOGHENE, in the department of computer Science the Faculty of physical science, University of Benin.

....

Pro. Mrs. Konyeha. Date

(Project supervisor)

APPROVAL

This project work is thereby approved by the department of computer science,

Faculty of physical science, University of Benin City, in partial fulfilment for the award of bachelor of science (BSC) degree in computer science.

....

Prof.(Mrs) Susane konyeha Date

(Project supervisor)

……

Prof. G.0. Ekuobase. .....

(Head of Department) Date

ACKNOWLEDGEMENT

I wish to appreciate and give thanks to God almighty for his abundance grace,

Protection throughout the period of study. I sincerely acknowledge with great

Gratitude to my supervisor prof. Mrs. Konyeha for her support, encouragement,

Suggestion, advice and time she spent putting me through in this project despite her busy schedule, I also express my gratitude to all my lecturers in computer science

Department prof. G.O. Ekuobase, prof. Frank Amadin, Mr S.O.P Oliomogbe,

Prof. A.A Imiavian , Dr kc Ukaocha, prof. Mrs Osunbor , Mrs O. Aziken, Dr

Mrs R.O Osaseri, prof. A.0 Egwali, Mr K.O. Otokiti, Mrs R.A Usiobaifo, Dr

Obi, prof. Mrs Egbokhare, prof. (mrs) Akwukwuma, Mr adetayo, Mr Obayagbona,

Mrs E.E Obasohan, Mr E.C Igodan, prof. Mrs S.C chiemeke, Mr F. Osagie, Mr

E.Nwelih, Dr E.P Ebitomere, Mrs .N.E.O Agbonlahor, Mrs T. Agenmonmen, Mr

Ojo solomen for all their support throughout my time in the department of

Computer science.

My family especially, my parents Mr And Mrs. Ejohwomu omare for their

Financial support and words of encouragement, and also to my siblings and my

Friends for their love and support, God bless you all.

CHAPTER ONE

INTRODUCTION

Background of the study.

With the advent of the internet, communication has taken a whole new dimension, reaching an ever-increasing audience worldwide since the late 1980s. Through the development of sophisticated technologies, a truly global network has been created with relatively low cost of entry. Communication is made easier through internet technology across borders, to an almost limitless audience. In addition to being a fundamental human right, Internet technology has numerous advantages, including its unique ability to share information and ideas. The same technologies that has help to facilitate such communication is now been used for internet misconduct or cybercrime.

Cybercrime can be defined as criminal activity involving an information Technology infrastructure , including illegal access (unauthorized access), Illegal interception (by technical means of non-public transmission of Computer data to, from or within a computer system), data interference (Unauthorized damaging , deletion deterioration, alteration or suppression of Computer system by inputting , transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), And electronic fraud.

The only variation is that it is conducted through a network, but its seriousness is on par with other types of crimes. Denial of service attacks, defaced websites, and computer viruses are making headlines in the news media.

Many other cyber-crimes that are not disclosed remain private. Despite the long existence of cybercrime, there was a lack of awareness about it.

The internet's global popularity has resulted in an increase in computer crimes,

Money laundering, fraud, software pirating, and corporate espionage, to name a

Few. Frustration among law enforcement officials stems from legislators' inability,

To stay ahead of rapidly advancing technology, cybercrime legislation needs to be updated, legislators face the need to balance the competing interests between

Individuals rights, such as privacy and free speech, and the need to protect the

Integrity of the world's public and private network.

The issue of legal jurisdiction complicates cybercrime enforcement further.

It takes more than one country to effectively pass pollution control legislation. Despite serious discussions within major international organizations, some countries do not prioritize combating cybercrime due to differing values or more immediate social issues.

Never before has it been this simple for a crime to be committed in one jurisdiction, giving cyber-criminals a safe haven, the purpose of this project work is to highlight cybercrime issues in Nigeria. And what the government is doing by way of law enacting and implementation to reduce cybercrime. It will also attempt to take a cursory look at how this crime is committed and how People can protect their selves from becoming victims.

1.2 Aim and Objectives of the Study.

The objective of this project is to bring attention to cybercrime issues in Nigeria and evaluate the efficiency of existing laws for offenders.

In addition to examining how and in what forms crime occurs, this project work will also explore the different forms of crime.

1.3 Scope of Study

We are focusing on crimes committed over networks with the following characteristics

1.4 Significance of the Study

This work will bring awareness about cyber-crime, its effect how most of the Cyber-criminal activities are carried out and what the government is trying to do to Reduce it. It will significantly act as a kind of yardstick to examine whether the Government has done enough by way of legislation to punish cyber-criminal and Curb their activities. Also, in a country like Nigeria where it is generally believed That cyber criminals are many, it is important that a study like this be carried out Periodically.

1.5 Methodology

For the purpose of this project, educational materials, directly and indirectly related To the topic at hand will be reviewed in order to make this study theoretical. Questionnaires will be used for the purpose of data collection from a target Population of different age groups and educational background who use the Internet often to sample opinions.

1.6 Limitation of study

In the course of this study, some limitations were encountered which include:

1. Lack of properly documented cases of cybercrimes that have taken place
2. Inability to get accurate details of when and how some of the laws for Punishment of cyber criminals have been enforced.
3. Time frame for the project work did not allow for in depth survey and analysis About cybercrime and criminals. Academic workload was also a limiting factor.

CHAPTER TWO

2.0 Cyber Crimes

An internet misconduct or cybercrime is a crime committed by using a computer or related device over a network without authorization. Using content or services that are forbidden or generally regarded as a crime constitutes cybercrime. (Ayinde, O. And Maitanmi (2013) define cybercrime as a crime committed on the internet. Internet misconduct may take different shape depending on the level of Understanding of the perpetrators and the nature of the' business' to be transacted the process. In every crime committed on the internet, the computer.

Cyber stalking, for example, and hacking, both involve attacking the computer, but the main target is the victim, not the computer (Okeshola F.B. and Adeta A.K 2013). In many cases, overlapping occurs and a perfect classification system is impossible. In situations where the individual is the main target, it is better to consider the computer a tool than a target. Create a detailed analysis of the vulnerabilities that are typically exploited by human perpetrators, focusing on their psychological and intangible impact, and explore the challenges faced in taking legal action against such individuals. Additionally, examine the underlying concept and motives behind these actions, highlighting that despite the evolution of tools and methods, the core essence of criminal behavior remains unchanged, making it crucial to understand the implications of these advancements in order to effectively combat them.

Cybercrime legislation can be challenging due to the fast pace of technological advancement and the need to balance individual rights with the protection of networks. Furthermore, legal jurisdiction becomes a complicating factor in enforcement efforts. Collaboration between nations is crucial as cybercrime knows

no boundaries, and one country alone cannot effectively address the issue. Cooperation between nations is necessary to develop comprehensive laws and enforce them globally.

Not all countries share the same level of urgency in combating cybercrime, and this can create challenges in addressing the issue effectively. Different values, priorities, and social problems can contribute to varying levels of commitment to combating cybercrime. This can create a safe haven for cybercriminals to operate, as they can exploit the differences in jurisdictions and hide behind them. International organizations like the OECD and G-8 are actively discussing cooperative schemes to address these challenges, but it will require continued effort and collaboration from all nations to effectively combat cybercrime and close these safe havens.

2.1 Cybercrime and criminality in Nigeria

Crime poses a significant obstacle to development for a nation. High levels of crime can hinder economic growth and have negative social consequences. Crime drains resources, undermines trust in institutions, and creates an unsafe environment for businesses and individuals. The presence of crime can deter investors and impede progress in various sectors, such as tourism and foreign direct investment. Therefore, it is crucial for nations to adopt effective strategies to combat crime and create a safe and secure environment that promotes development.

For Nigeria, in the battle against cybercrimes, efforts are now being directed at the source and channels through which cybercrime are being perpetuated the most popular one being internet access points aided by intensive ISPs. Majority of the cyber-crime perpetrated in Nigeria generally are targeted at individuals and not necessarily computer systems, hence they require less technical expertise on the part of these criminals (Peter Grace, D. 2001) When human faults such as greed and inexperience are used on a wide scale, the consequences may be seen in the real world .The primary damages incurred are of a psychological and economic nature through the internet, the same criminals or persons with criminal intent have simply been given a tool which increases their potential pool of victims and makes them all harder to trace and apprehend. The cybercriminal needs to see the path of crime ahead of him free of obstacles in addition to his own mind set and the

strength of his motivations. If every single person were to place obstacles of their own, no matter how small, the criminal path would appear to be far less lucrative in the eyes of even the most desperate criminal. Except in a few cybercafés where content filters are downloaded and installed to filter undesired internet material, Nigeria's efforts to combat online pornography have not made much progress. Beyond his own mind set and the intensity of his motivations, the cybercriminal needs to see the path of crime unobstructed. If every single person were to place barriers in the way of their own criminal activities, no matter how minor, the criminal path would appear far less lucrative to even the most desperate of criminals. With the exception of a few cybercafés where content filters are downloaded and installed to filter undesired internet material, Nigeria's efforts to combat online pornography have not made much progress. Interested parties who are able to pay for a fixed wireless internet connection can now carry out their wicked deeds from the comfort of their own homes. This explains why society and the globe at large are ill-equipped to deal with them.

2.2 The Nature of cyber-crime in Nigeria. The following categories of crime are the most common ones in Nigeria cyber space.

(a)Huckster

The hallmarks of the hucksters include a protracted period of time (usually at least a month) between harvest and first message, a high volume of messages sent to every harvested spam-trapped address, and a propensity for product-based spam (i.e., spam that offers a real product for shipment or download, even though the product is fake).

(c)Fraudsters

The fraudsters are distinguished by their almost instantaneous turnaround time (usually less than 12 hours) between harvest and first message; only a small number of messages (e.g., phishing: Advanced fee fraud 419 from the Nigerian perspective) are sent to each harvested address. Fraudsters frequently gather email addresses and send everyone a single message at one specific time. The mailing address extractor is the main tool for obtaining addresses.

(b) Piracy:

The illegal duplication and distribution of video games, audio CDs, software applications, and movies is known as piracy. There are several ways to go about this. Typically, pirates purchase or download the original versions of software, movies, or video games from the internet. They then unlawfully distribute these copies online so that other people can download and use them without the original software owner's consent. This is referred to as warez, or online piracy. While contemporary piracy may not be as dramatic or thrilling, the financial losses suffered by the victim are far more subtle and extensive. Since it appears that the average person is also benefiting from this particular type of cybercrime, it might be the most difficult to combat.

(d)Hacking:

Every day, young Nigerians can be seen participating in brain storming sessions at cyber cafes as they attempt to decipher security codes for websites that sell products online, process ATM cards, and conduct e-commerce. What's surprising is that they produce results despite having little formal education and little comprehension of the complexities of computing techniques! Phishing is also growing in popularity as thieves pretend to be product websites in order to trick unsuspecting users into placing orders for goods that do not actually exist.

2.3 Nigerian cyber criminals, How they operate.

The typical cybercriminal is not a computer whiz kid or a seasoned professional programmer with extensive computer knowledge. When it comes to computer use, their literacy level is typically mediocre. Online crime was a topic of discussion on Oprah Winfrey's popular American talk show, which was hosted around the same time in 2007. It became evident that day how the outside world viewed Nigeria. .. This one-hour talk show unfairly embarrassed the nation. That was a day the country will never forget. Cybercrime victims appeared on the program to share their stories, and surprisingly, the majority of them held Nigerians responsible for their misfortunes. Firm action should be taken on this issue because the nation is suffering from its effects. The difficulty the average Nigerian has obtaining a visa

to visit or study in nations like the United Kingdom is another effect of this. Nigeria currently ranks among the most corrupt nations in the world, and it will never reach its full potential. A typical Nigerian cyber criminals needs a few things to carry out business. These include;

1. Internet connection
2. E-mail address
3. E-mail extractor
4. E-mail account.

1. Internet connection: As time is money, this should go rather quickly. Internet cafes are the best and most economical place to do this. Shady internet cafes can be found in many states of Nigeria, serving cybercriminals and providing them with internet access. Festac and similar areas are well known for this. These cybercafés have a method for doing that. When night falls, they close the doors, but they leave them ajar for criminals to operate fearlessly. One would assume that the proprietors of these internet cafes get a cut of the loot that these criminals accumulate. After making a good living, some criminals would advance to buying their own internet connection so they could work from home. This makes it more difficult for law enforcement to find them because security personnel lack the tools needed to monitor such an internet connection.

2. **E-mail address**: These are typically gathered from online forums where participants post their email addresses, large company business cards, and other information. The most widely used method of email address hacking involves

cybercriminals sending chain letters to potential victims' email accounts. The way these letters are written is meant to give victims the impression that the writer is someone they are not. The chain letter sample that follows is an example of this type.

CENTRAL BANK OF NIGERIA OFFICE OF THE PRESIDENT,

THE HONOURABLE, GOVERNOR OF CBN. MAYFAIR GUARDEN, LAGOS NIGERIA, Date 13th October, 2019.

Official web Account: Olayemi Michael cardoso 123@i13.com.

Our Ref: *CBN/OHG/OXD1/2019.* *Your Ref……*

TELEX: CENTRAL BANK

PAYMENT FILE: CBN/BEN/13.

Attn : sir/madam,

PAYMENT NOTIFICATION OF YOUR FUNDS.

I am aware that you will be surprised to receive this letter. First of all, allow me to formally introduce myself as the executive governor of the Central Bank of Nigeria (CBN), Dr.Olayemi Michael Cardoso. Since you failed to submit your claim as the

correct beneficiary, your inheritance funds were redeposited into the CBN "federal suspense account" last week, and as a result, I have officially contracted with you. As you may be aware, all commercial banks in Nigeria are subsidiaries of the Central Bank of Nigeria.

I must admit that I was surprised by these men because I had to question them about why they had come to see me in person. They stated that they were present on your behalf to retrieve the inheritance bill sum of (U$$ 3,000,000) that is legally yours. In light of this development, I questioned them about who gave them permission to travel to Nigeria in order to collect the funds on your behalf. Actually, this was the largest surprising that this bank has received money on account of your inheritance even though it is still in the "Federal suspense Account" of CBN. You sent these men to retrieve the money without telling us. The reason you sent these men to come collect your funds on your behalf is beyond us at this bank. In your capacity as this bank's executive governor, you ought to have at least told me if you truly wanted them to assist you in getting your inheritance, Bill Sum. They submitted several important documents that attested to the fact that you did, in fact, send them for the purpose of collecting the funds. To be honest, I find it extremely confusing that you made this decision without consulting me. These are the documents that they tendered at Bank today.

1. *LETTER OF ADMINISTRATION*
2. *HIGH COURT INJUCTION.*
3. *ORDER TO RELEASE.*

In actuality, the documents they submitted to the bank serve as unequivocal evidence that you instructed them to retrieve the funds on your behalf. When we finally told them to return the following morning, they made a promise to do so. I was meant to give this fund to them in my capacity as governor of the Noble Bank, but I held off because I wanted to speak with you first. Owing to the nature of my work, I don't want to release these funds to anyone other than the designated beneficiary in error. Please enlighten us on this matter before we pay the foreigners who came on your behalf. Upon receiving this private correspondence, you must call the Bank immediately you receive this confidential Letter.

2.4 The Role of the Government.

The Nigerian government has implemented several measures to curb the proliferation of cybercriminals and their illicit activities, realizing the threat they pose to the nation's development. The Corrupt Practices and Other Related Offences Act of 2000 was enacted as a result of Nigeria's determination to battle and prevail against corruption and cybercrimes. Olusegun Obasanjo, who was the president at the time, introduced the Act as the first bill to the National Assembly for consideration in anticipation of the democratic administration in T999.

The 13th of June, 2000 saw the passing and signing of the act. The Independent Corrupt Practices and Other Related Offenses Commission (CPC), an annex body charged with igniting corruption and other related offenses, is established by the Act. On September 29, 2000, the ICPC was officially established.

An additional of these laws was the one that established the EFCC in 2004 and gave it the authority to fight financial and economic crimes. The Commission is tasked with upholding the terms of other laws and regulations pertaining to economic and financial crimes, such as the Economic and Financial Crimes commission Establishment act (2004), and has the authority to prevent, investigate, prosecute, and penalize economic and financial crimes.

>The Money Laundering Act 1995

>The Money Laundering (Prohibition) act 2004

>The Advance Fee Fraud and Other Fraud Related Offences Act 1995

>The Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994

The EFCC has an anti-cybercrime unit that is intended to deal with and eradicate cybercrimes within Nigeria. It is mandated by the Banks and Other Financial Institutions Act of 1991 and the Miscellaneous Offenses Act. While some cybercriminals have been apprehended and prosecuted by the EFCC and ICPC, much more work needs to be done before cybercrimes are completely eradicated. It is the social duty of the government to provide job opportunities and jobs to its citizens. It's common knowledge that most criminals will choose a better option before turning to crime. The government needs to make sure that conditions are Favourable for people to succeed in areas of life other than crime in order to discourage people from turning to cybercrimes and other vices. This is due to the fact that people are more likely to engage in activities where they are certain to receive compensation commensurate with their inputs than what most cybercriminals receive.

CHAPTER THREE

3.0 Research Methodology

3.1 Population Design.

People living in Edo state's Benin City made up the sample. Among the 300 participants in the study, all of them were computer literate. The respondents were chosen at random from various locations.

3.2 Instrument

The survey design is used in this study. This was selected because it typically polls a subset of the general public about their opinions on cybercrimes in Nigeria, their level of computer literacy, and their usage patterns of the internet. The purpose of the questionnaire was to provide us with secure responses to particular inquiries.

Grown in this research project. Relevant data in the following areas was requested in the questionnaire:

i. Knowledge about computers.
ii. Awareness about the internet.
iii. Awareness about cybercrimes.
iv. Government intervention in cybercrimes as it affects Nigeria.
V. Ways of reduction of cybercrimes in Nigeria.

Vi. Efficiency of the economic and financial crime commission (EFCC) and related bodies. The required data did not include personal information, but covered computer and internet literacy, frequency of use, encounters with cybercriminals, and suggestions for reducing cybercrime in Nigeria. Judgments were made based on different responses ranging from yes, no, undecided and I don't know and also choose from other list of options.
Respondents were asked to indicate their sex, age range and educational level.

3.3 Description of the Instrument:

In order to gather information for the study. Surveys were employed. The purpose of the questionnaire was to find out if the respondents used the internet, why people fall prey to cybercriminals, and why Nigerians engage in cyberattacks. There were twenty questions on the survey, each consisting of three or more options from which respondents can select. After carefully reviewing the questionnaire, my supervisor decided it was appropriate. To produce the necessary data so that the study can fulfil its intended purpose.

3.4 Data Collection:

Visits to resident halls and offices were used to gather data from respondents. Employee offices, cyber cafes, and some people's arbitrary approach in Benin City. Edo state of Nigeria.
While some questionnaires took several days for respondents to complete and return, the majority were distributed and collected almost instantly. While some individuals understood the seriousness of the questionnaires, others needed guidance on how and why to fill them out honestly. Data from the questionnaires was gathered and converted into information based on how they were completed.

3.4.1 Questionnaire:

This is the list of inquiries intended to look into a specific topic.

Researchers (me) use questionnaires to gather information about past, present, and anticipated events; conditions influencing past, present, and anticipated events; and viewpoints, opinions, decisions, and options.
Respondents may receive questionnaires via direct mail delivery or by Make contact. The direct contact method was applied in this investigation. This was employed since the majority of the research was conducted in Benin City. An attachment to this work is an appendix containing a copy of the questionnaire used.

3.5 Validation of the Instrument:

The research instrument (questionnaires) was developed by me, the researcher, and then submitted to the project supervisor for validation.

3.6 Sample and Sampling Procedure:

The study's samples consisted of 300 respondents, including regular people and on-the-spot computer and internet users.

- Uselu market.
- Computer Science Department, University of Benin.
- Chicken Republic, new Lagos road, Benin City.
- God is good motors.

3.7 Method Used In Data Analysis

A pie chart was utilized to visually represent the data when the simple frequency distribution table was used to analyse the data collected for this study.

To improve comprehension of the procedure, more explanation was provided.

Outcome. An attempt was made to provide a succinct explanation.

CHAPTER FOUR

4.0 Data Analysis

This chapter provides the data collected through the questionnaires administered to some persons to find out information on if and how they use web Browser .The respondents to the questionnaire were randomly selected. Also provided in this chapter is the percentage analysis and chart representation of the collected Data and their corresponding interpretations.

4.1 General Statistics on Questionnaire Administered

A total of three hundred (300) questionnaires were distributed to three hundred (300) respondents residing in Benin City, Edo state, Nigeria, the questionnaire was randomly distributed. However, out of the three hundred (300) copies of the Questionnaire distributed, three hundred (300) was filled and returned. To get l00% response rate for the research work.

A total of three hundred (300) questionnaires with 20 questions cache were used to carry out the analysis. The questions were analysed with statistical package for Social sciences (spss) as required for proper research work.

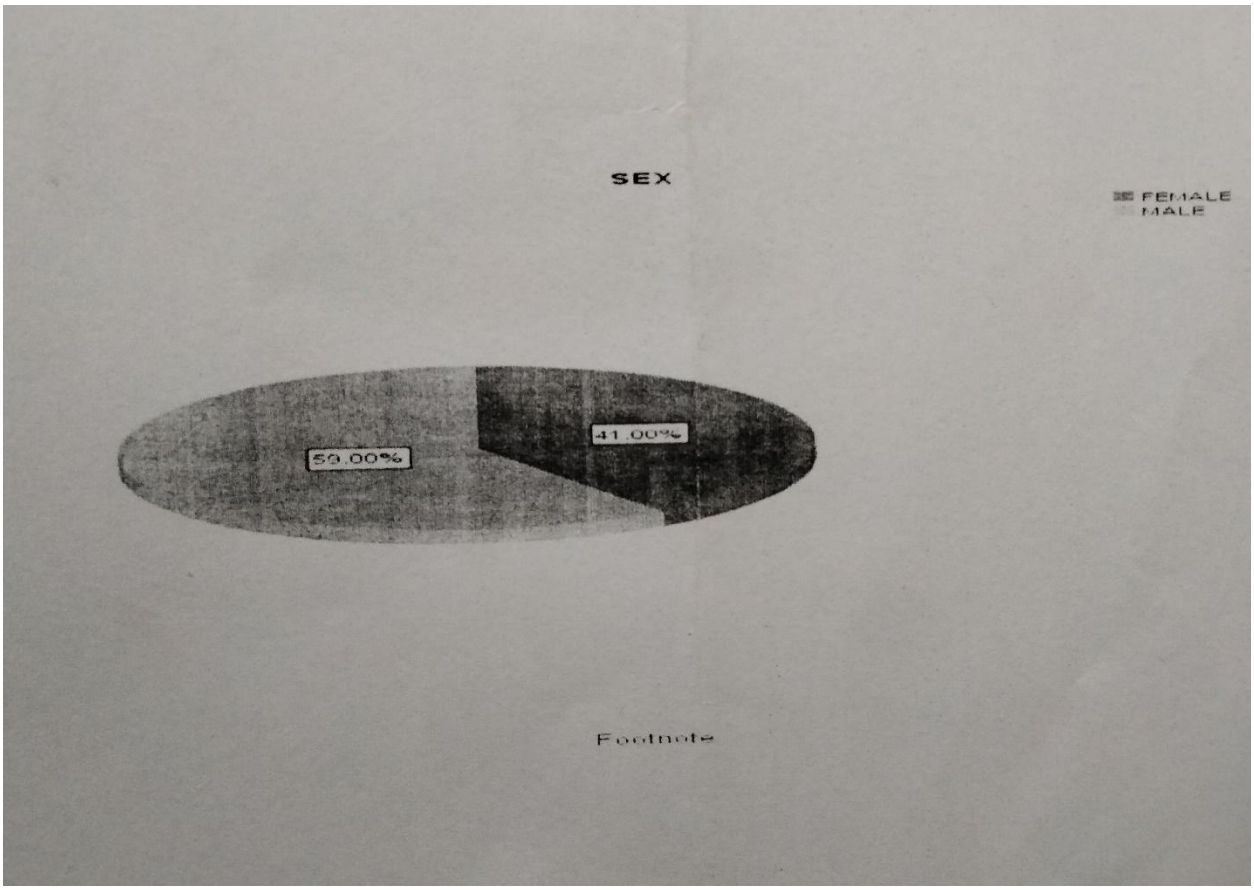
4.10 Analysis of the Questionnaire

4.1 Research Question 1: Sex

The first research question of the research instrument was sex to determine the number of males and females who responded to the questionnaire. The table is show below:

TABLE 4.1: SEX.

SEX	FREQUENCY	PERCENTAGE %
MALE	202	59%
FEMALE	98	41%
TOTAL	300	100



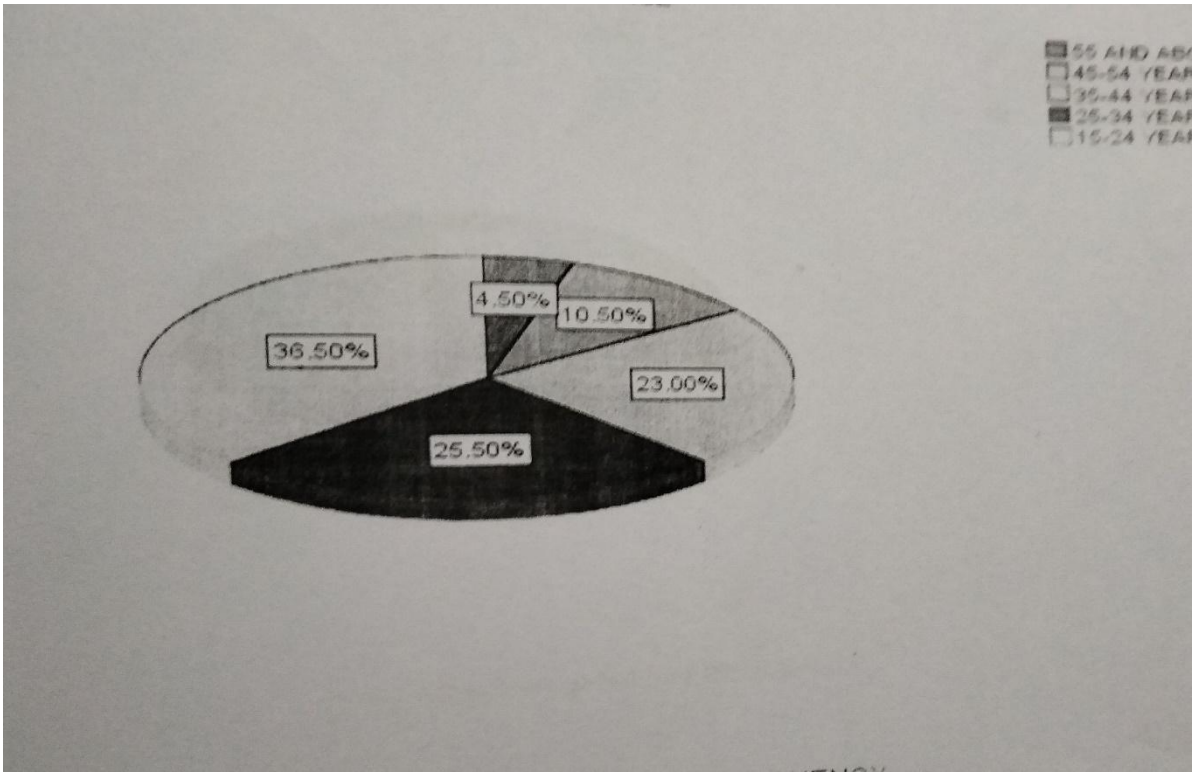
4.2 Research Question 2: Age

The second question of the grade of respondents and is captured in table 4.2 below.

TABLE 4.2: AGE

AGE	FREQUENCY	PERCENTAGE%
15-24	100	

25-34	98	25.50%
35-44	72	23.01%
45-54	21	10.50%
55 AND ABOVE	9	4.5%
TOTAL	300	100

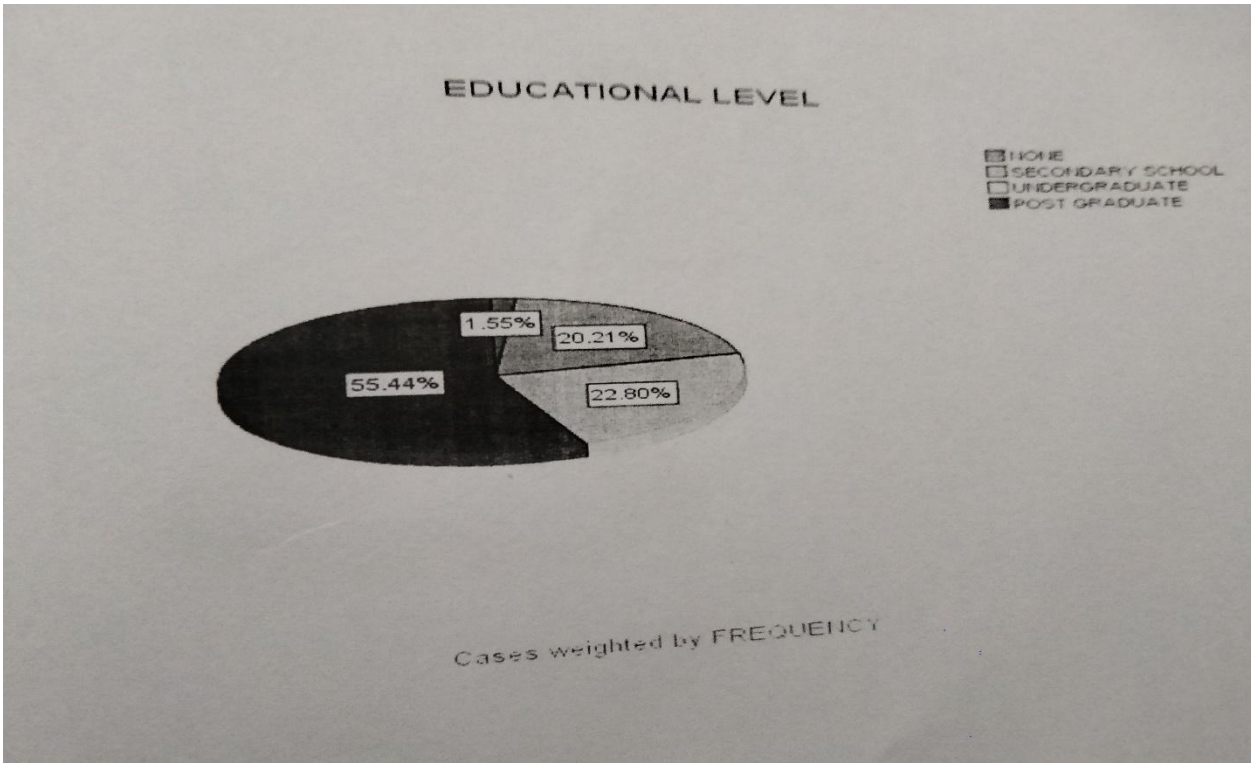


4.3 Research Questions 3: What educational level Are You?

Table 4.3: what educational level are u now?

EDUCATIONAL	FREQUENCY	PERCENTAGE%

LEVEL		
NONE	4	1.5%
SECONDARY SCHOOL	100	20.21%
UNDERGRADUATE	156	55.44%
POSTGRADAUTE	40	22.80%
TOTAL	300	100

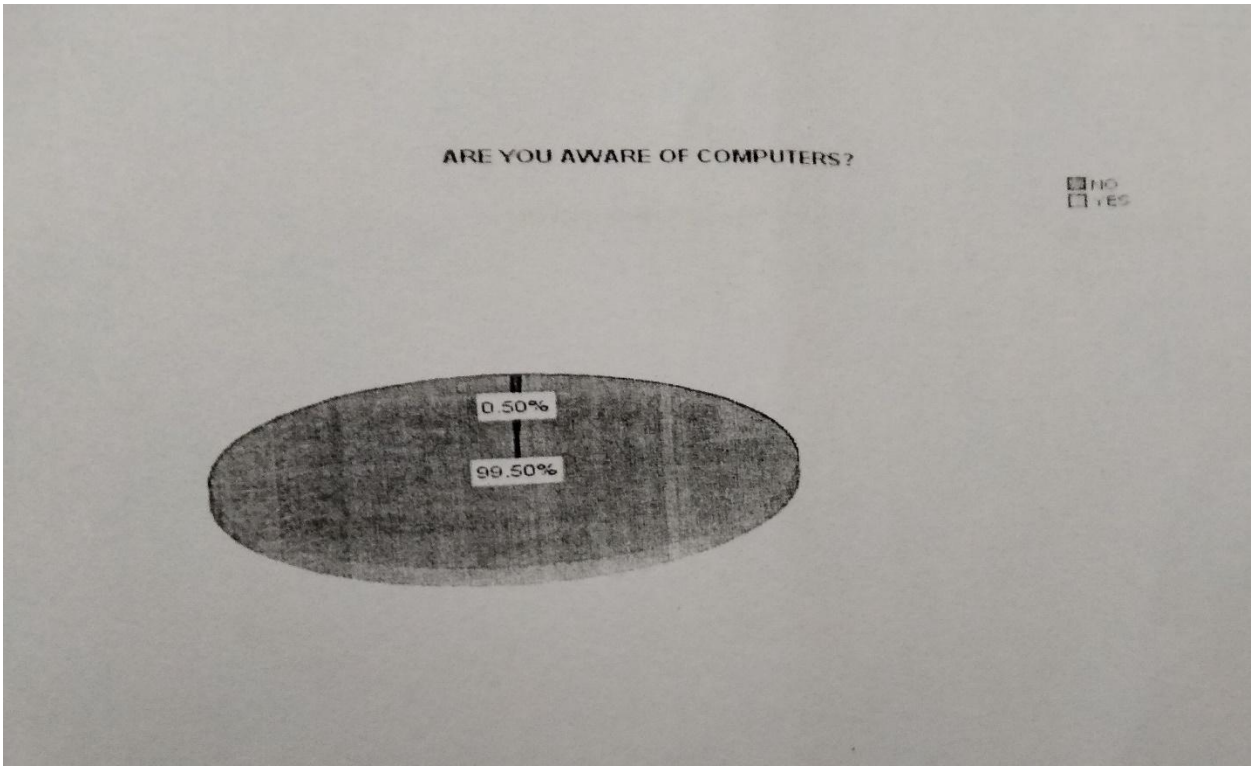


4.4. Research Question 4: Are You Aware Of Computer?

This research was used to determine the level of computer awareness possessed by the respondent to know if majority of them have an idea about the topic.

TABLE 4.4 Are You Aware Of Computer

ARE YOU AWARE OF THE COMPUTER	FREQUENCY	PERCENTAGE%
NO	1	99.50%
YES	299	0.50%
UNDECIDED	0	0.00
TOTAL	300	100

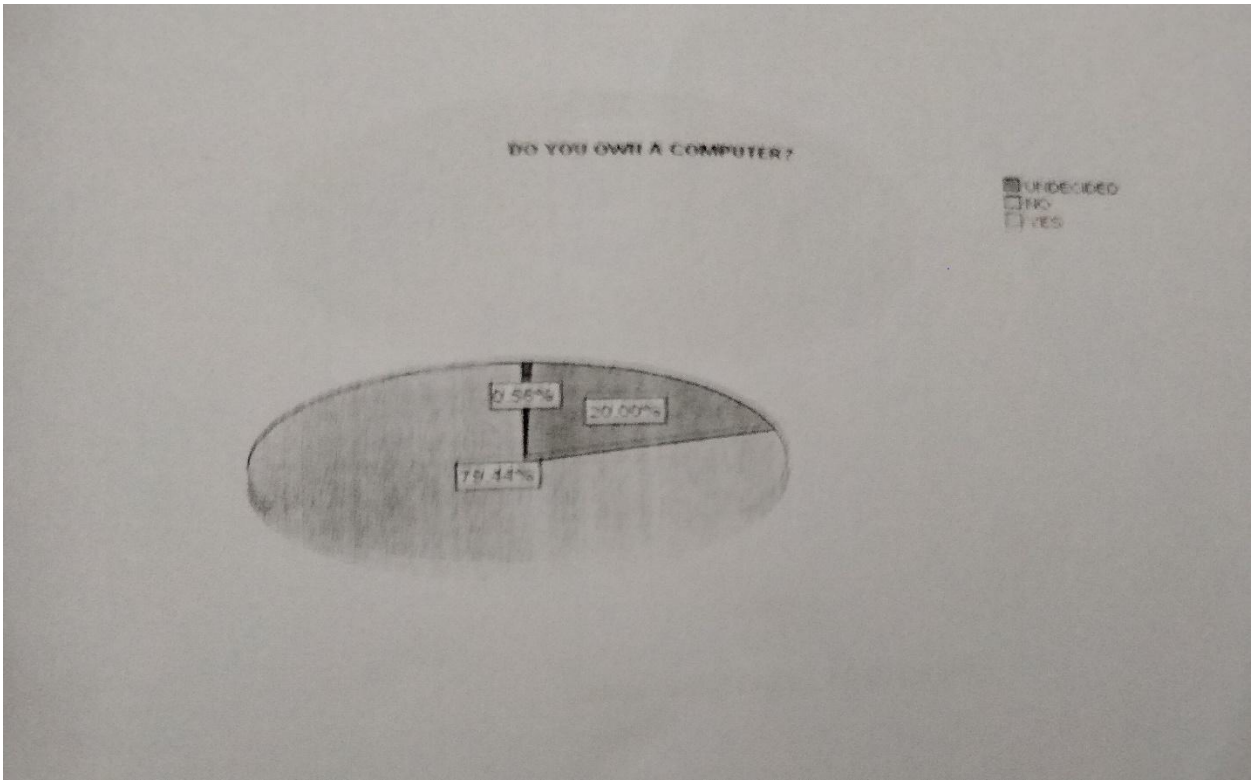


4.5 Research Question 5: Do You Own A Computer?

This research questions was used to determine number of respondents that own a computer system.

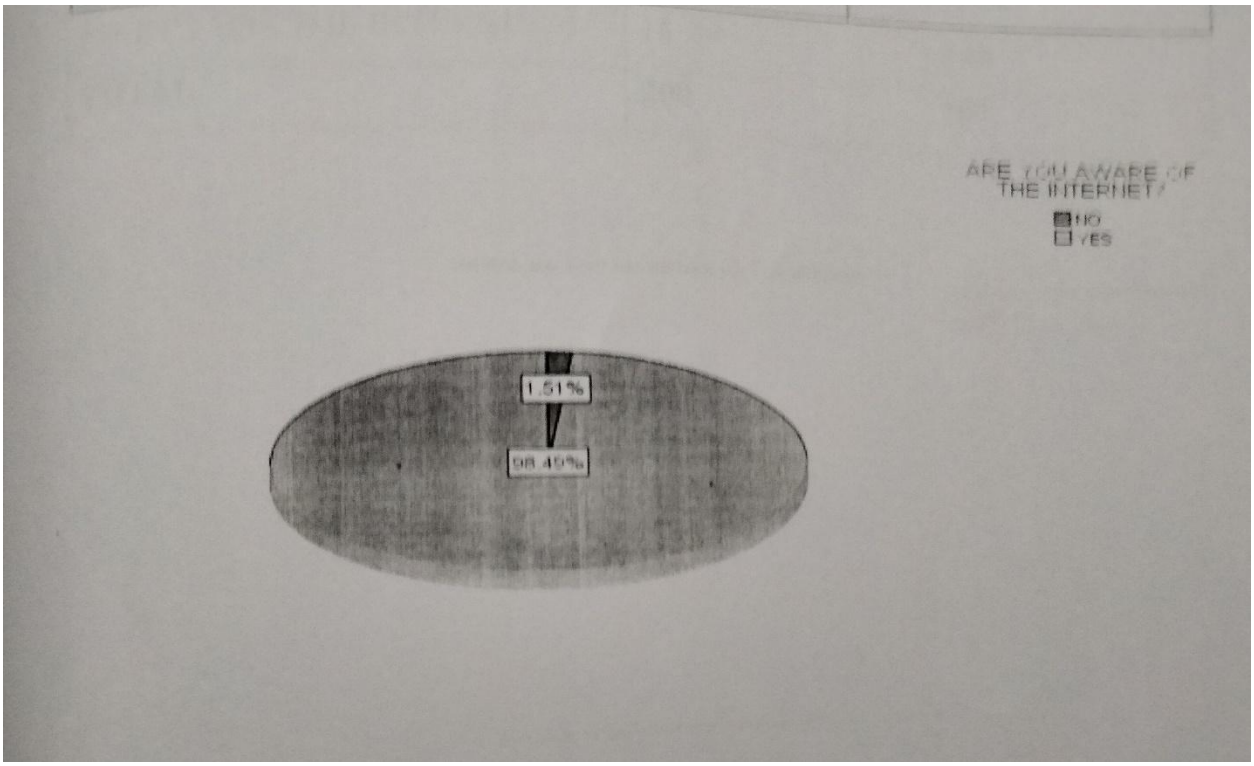
TABLE 4.5 DO YOU OWN A COMPUTER

DO YOU OWN A COMPUTER	FREQUENCY	PERCENTAGE%
YES	200	79.44%
NO	99	20.00%
UNDECIDED	1	0.56%
TOTAL	300	100



4.6 Research Question 6: Are You Aware Of the Internet?

ARE YOU AWARE OF THE INTERNET	FREQUENCY	PERCENTAGE%
YES	206	98.49%
NO	94	1.15%
UNDECIDED	0	0
TOTAL	300	100

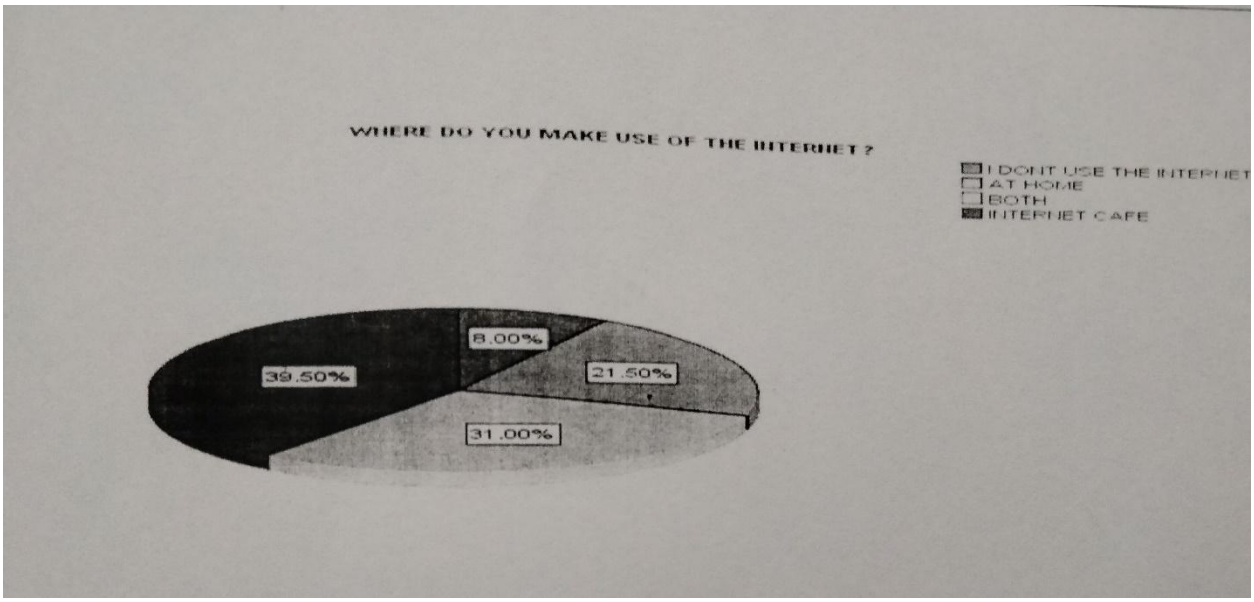


4.7 Research Question 7: Where Do You Make Use Of The Internet?

This research question was used to determine the number of respondents that actually make use of the internet from those that are aware of the internet.

TABLE 4.7.2 Where Do You Make Use of the Internet

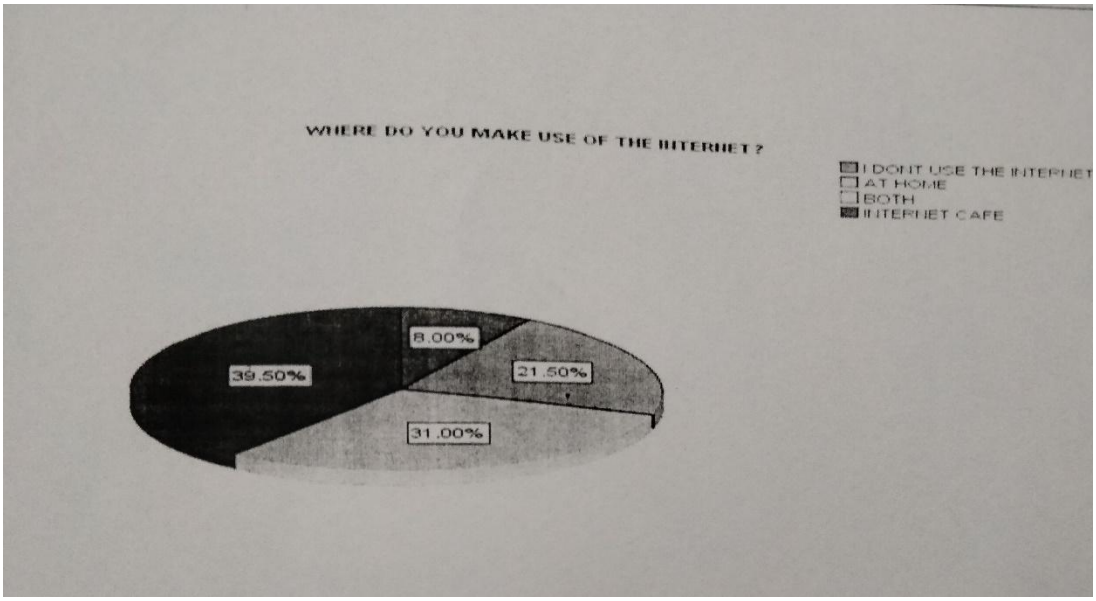
WHERE DO YOU MAKE USE OF THE INTERNET	FREQUENCY	PERCENTAGE%
AT HOME	150	21.50%
INTERNET CAFE	56	39.50%
BOTH	50	31.00%
I DON'T USE THE INTERNET	40	8.00%
TOTAL	300	100



4.8 Research Question 8: Do You Make Use Of E-mail?

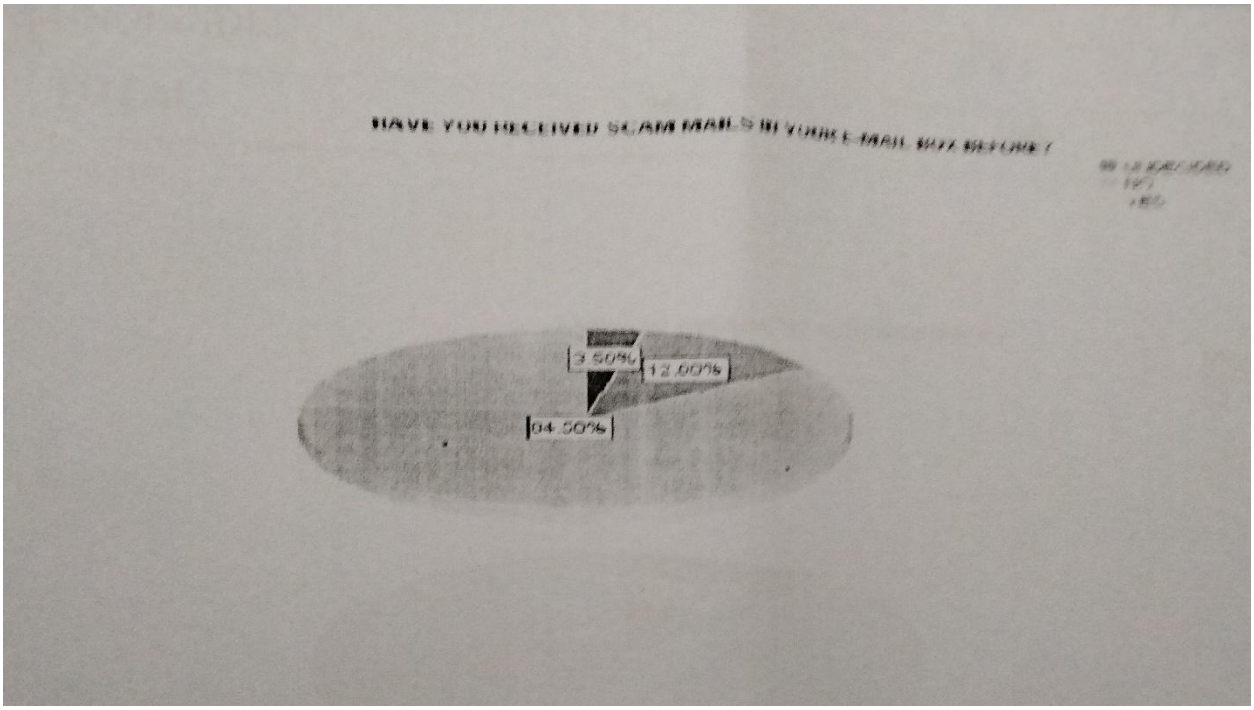
TABLE 4.8: DO YOU MAKE USE OF E-MAILS.

DO YOU MAKE USE OF E-MAIL	FREQUENCY	PERCENTAGE%
YES	260	87.00%
NO	30	11.50%
UNDECIDED	10	1.50%
TOTAL	300	1000



4.9 Research Question 9: Have you received scam Mails in your E-mail before.

HAVE YOU RECEIVED SCAM MAIL	FREQUENCY	PERCENTAGE %
YES	200	84.50%
NO	56	12.00%
UNDECIDED	44	3.50%
TOTAL	300	100

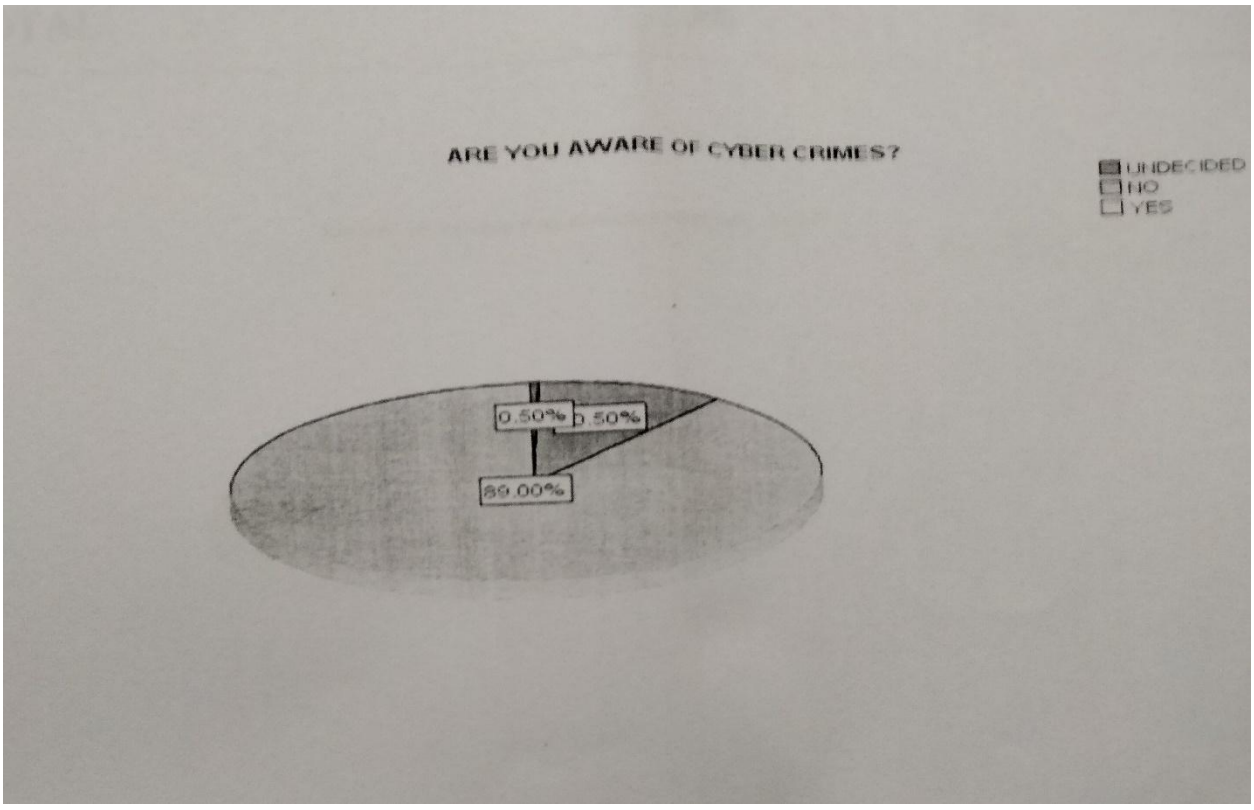


4.10 Research Question 11: Are you Aware of cybercrime?

This research question is used to determine the numbers of respondents that have awareness about the research study been carried out.

The result is show in the table 4.11

ARE YOU AWARE OF CYBERCRIME?	FREQUENCY	PERCENTAGE%
YES	200	89.00%
NO	99	10.50%
UNDECIDED	1	0.5%
TOTAL	300	100

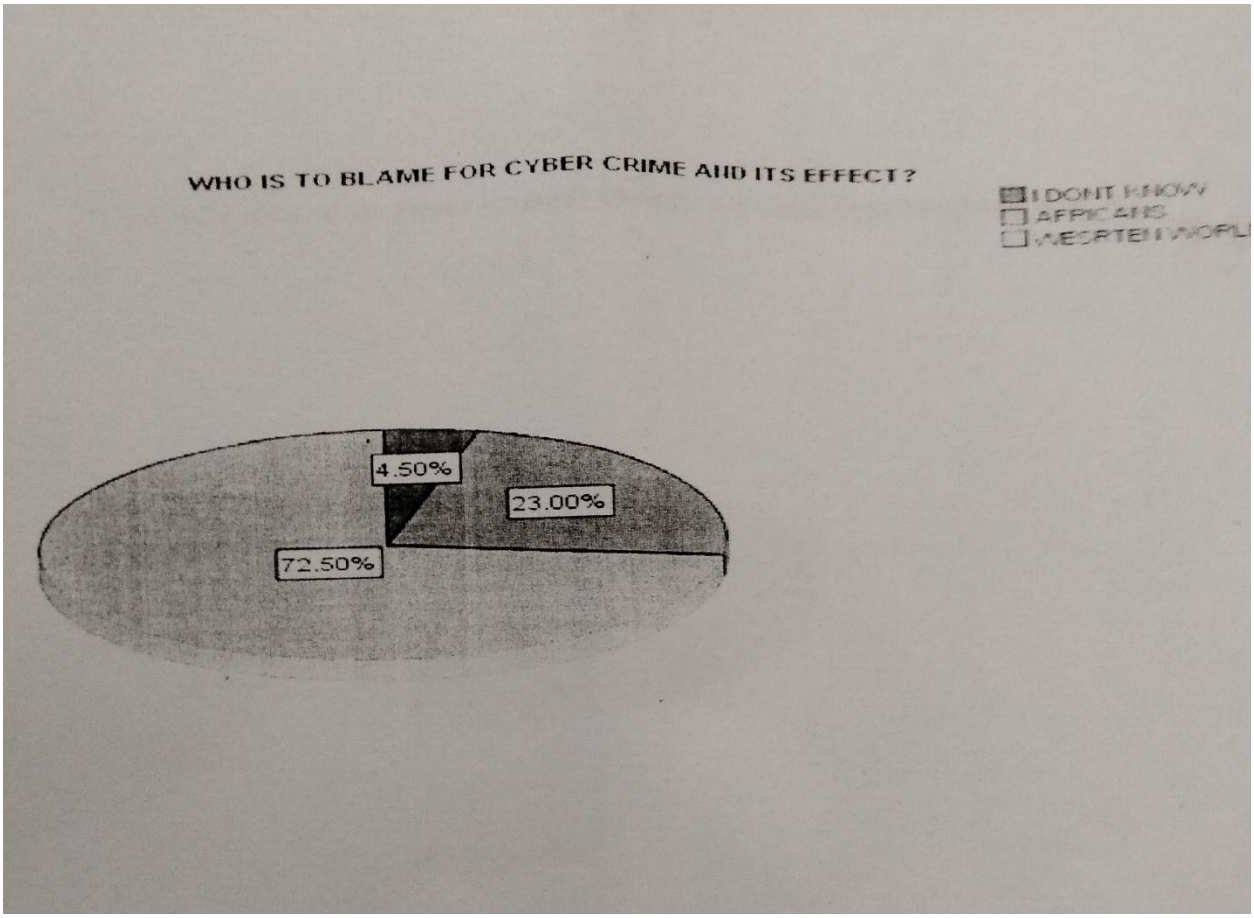


4.11 Research Question 12: Who Is To Be Blame For Cybercrime And Its Effects?

This research question is used to determine what our respondents think is responsible for cybercrime and its effects.

The result is shown in Table 4.12

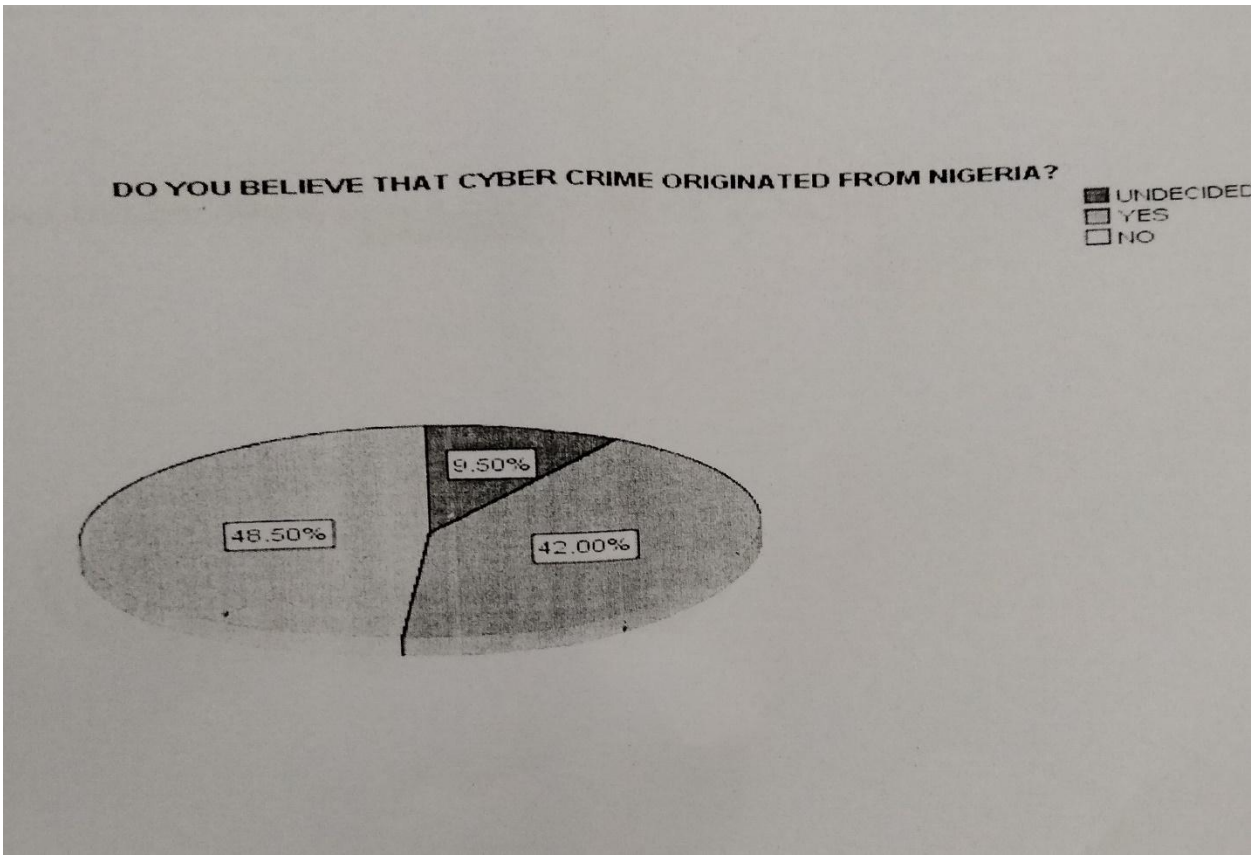
WHO DO YOU BLAME FOR CYBERCRIME AND ITS EFFECTS	FREQUENCY	PERCENTAGE %
AFRICANS	90	23.00%
WESTERN WORLD	190	73.50%
I DON'T KNOW	20	3.50%
TOTAL	300	100



4.12 Research question 12: Do you think cybercrime originated from Nigeria?

This research work was used to determine if respondents believed that cybercrime originated from Nigeria. It is shown in Table 4.13

DO YOU THINK CYBERCRIME ORIGINATED FROM NIGERIA	FREQUENCY	PERCENTAGE%
YES	180	42.00%
NO	80	48.00%
UNDECIDED	40	9.50%
TOTAL	300	100

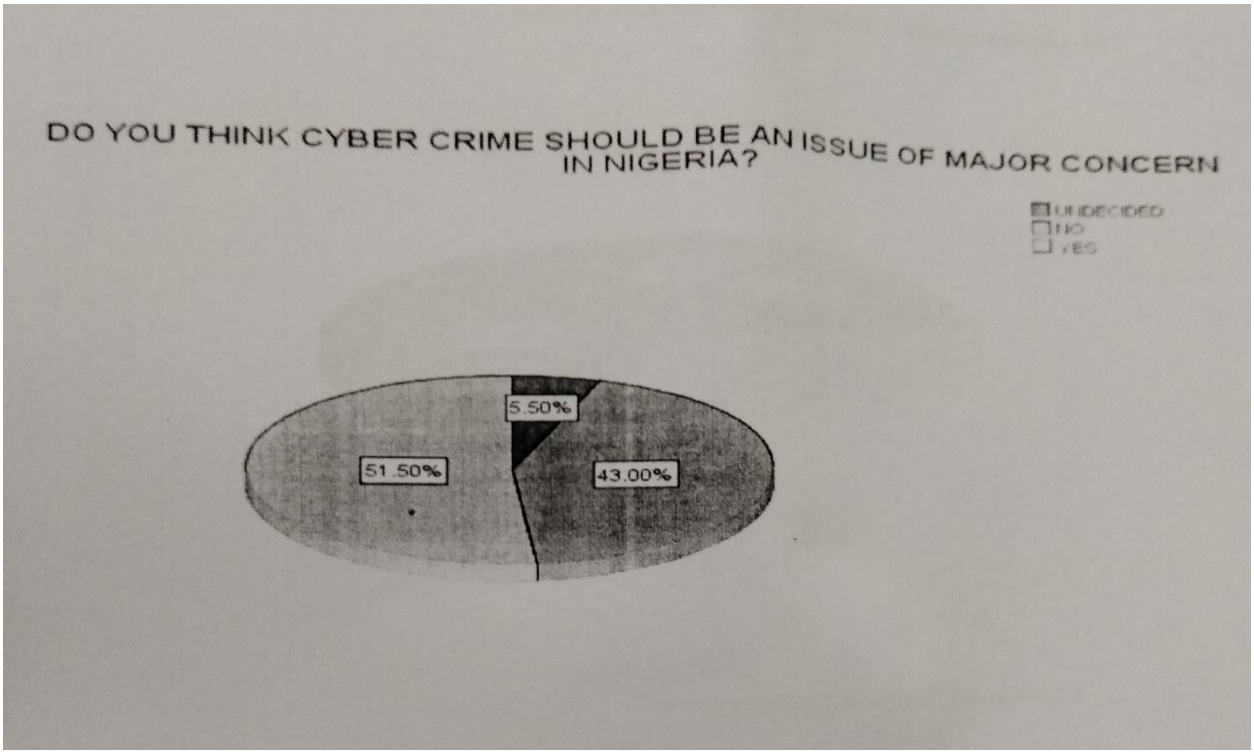


4.13 Research question 14: Do you think cybercrime should be an issue of major concern in Nigeria?

This research question was design to know if respondents feels that cybercrime should be taken seriously by the Government of Nigeria. The result is shown in Table 4.14

DO YOU THINK CYBERCRIME SHOULD BE A MAJOR CONCERN IN NIGERIA?	FREQUENCY	PERCENTAGE%
YES	194	51.50%

NO	86	43.00%
UNDECIDED	20	5.50%
TOTAL	300	100



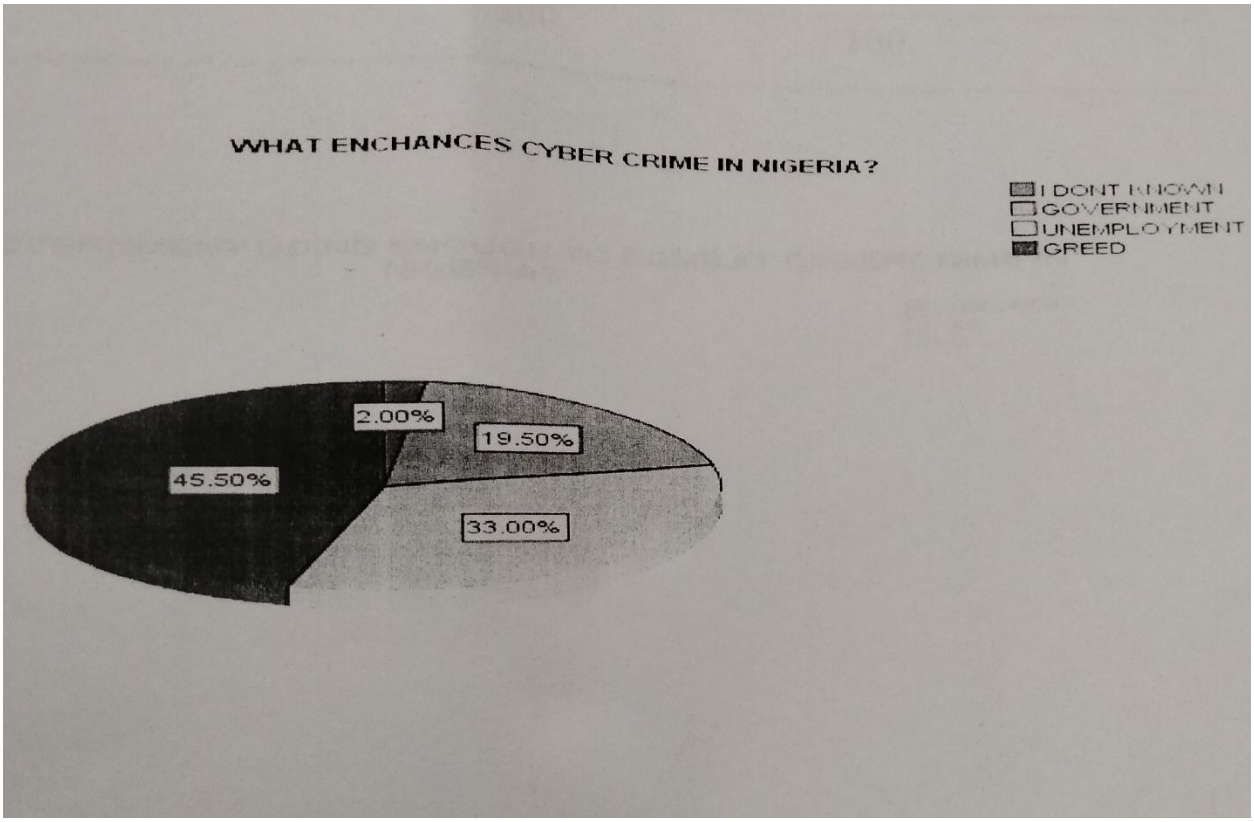
4.14 Research Question 15: What enhance cybercrime in Nigeria?

This project work is design for our research instrument to know what encourage cybercrime in Nigeria.

The result is shown in Table 4.15

WHAT ENHANCE CYBERCRIME IN NIGERIA	FREQUENCY	PERCENTAGE%
GOVERNMENT	150	19.50%
GREED	54	45.50%
UNEMPLOYMENT	86	33.00%

I DON'T KNOW	10	2.0%
TOTAL	300	100



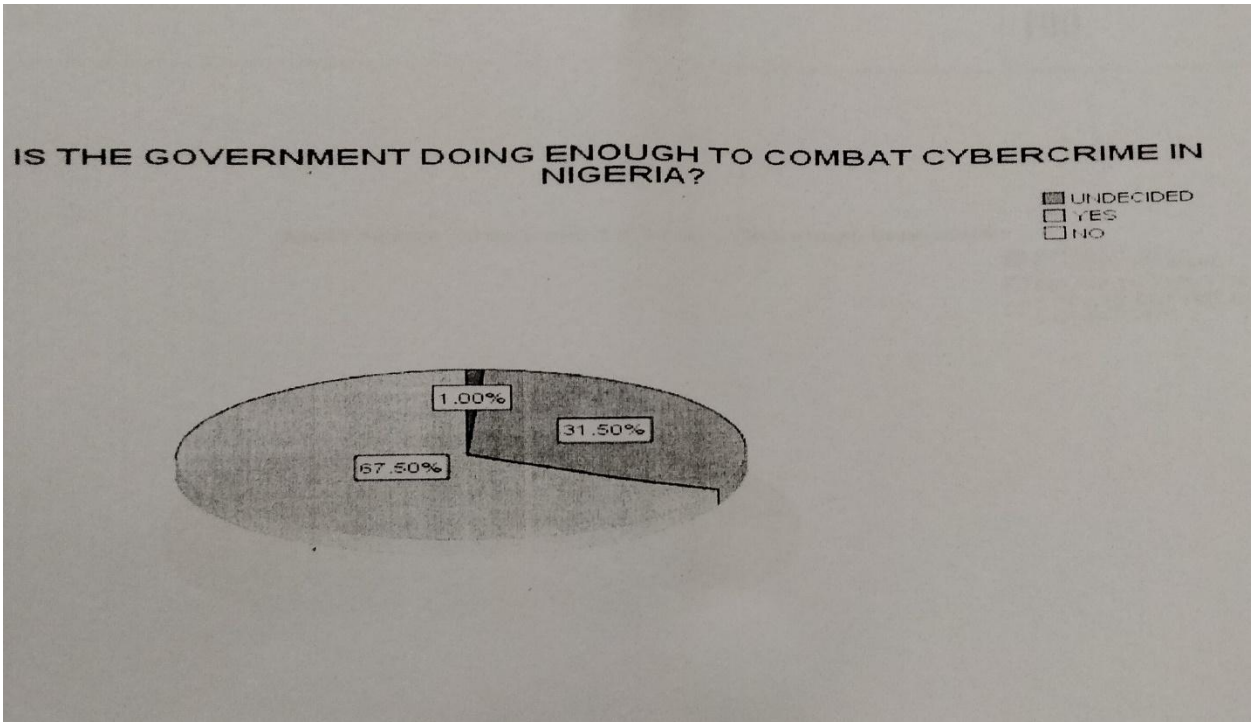
4.15 Research Question 16: Is the Government Doing Enough to combat cybercrime in Nigeria?

This question was design to know if the government is doing enough to reduce cybercrime rate in Nigeria.

The result is shown in Table 4.16.

IT'S THE GOVERNMENT DOING ENOUGH TO COMBAT CYBERCRIME IN NIGERIA	FREQUENCY	PERCENTAGE%

YES	90	31.50%
NO	200	67.50%
UNDECIDED	10	1.00%
TOTAL	300	100

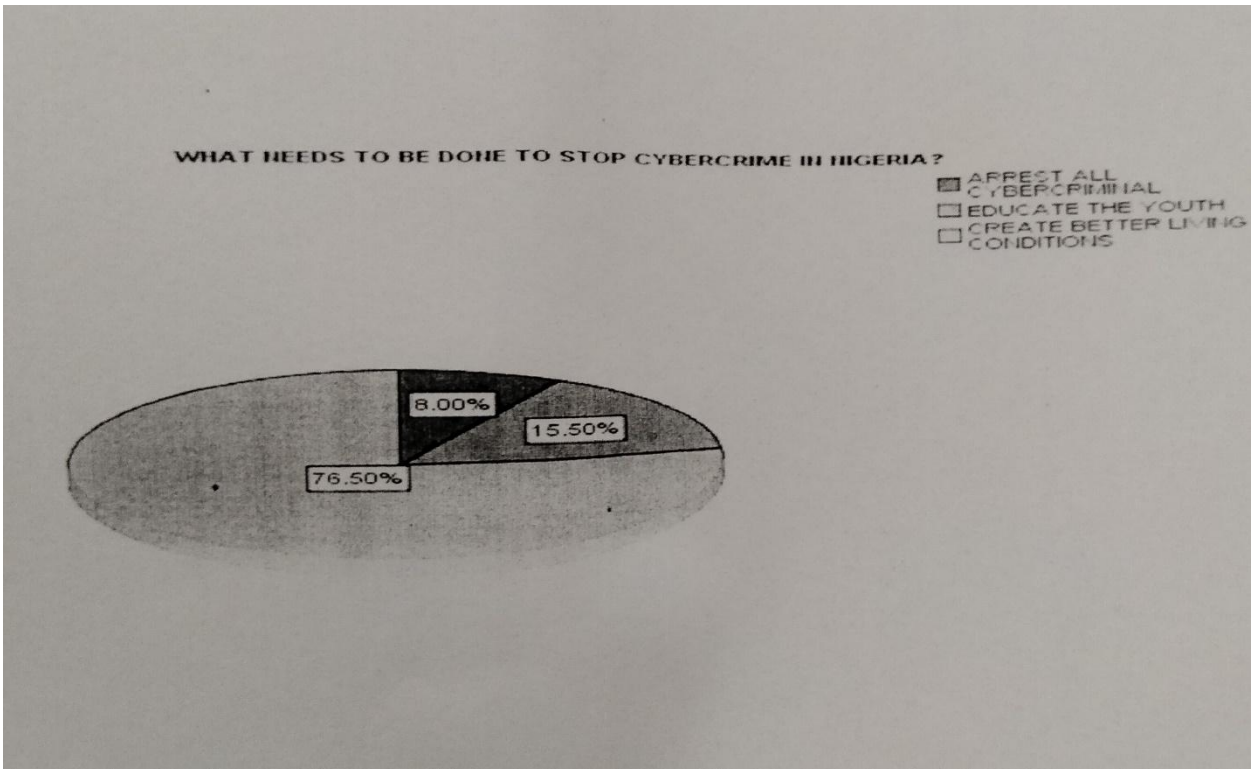


4.16 Research Question 16: What need to be done to reduce cybercrime in Nigeria?

This research work was design to determine what respondents think should be done to stop cybercrime in Nigeria? The result is shown in Table 4.17

WHAT NEED TO BE DONE TO REDUCE CYBERCRIME IN NIGERIA?	FREQUENCY	PERCENTAGE%
EDUCATE YOUTH	150	15.50%
CREATE BETTER LIVING	90	76.50%

ARREST ALL CYBERCRIMINALS	60	8.00%
TOTAL	300	100



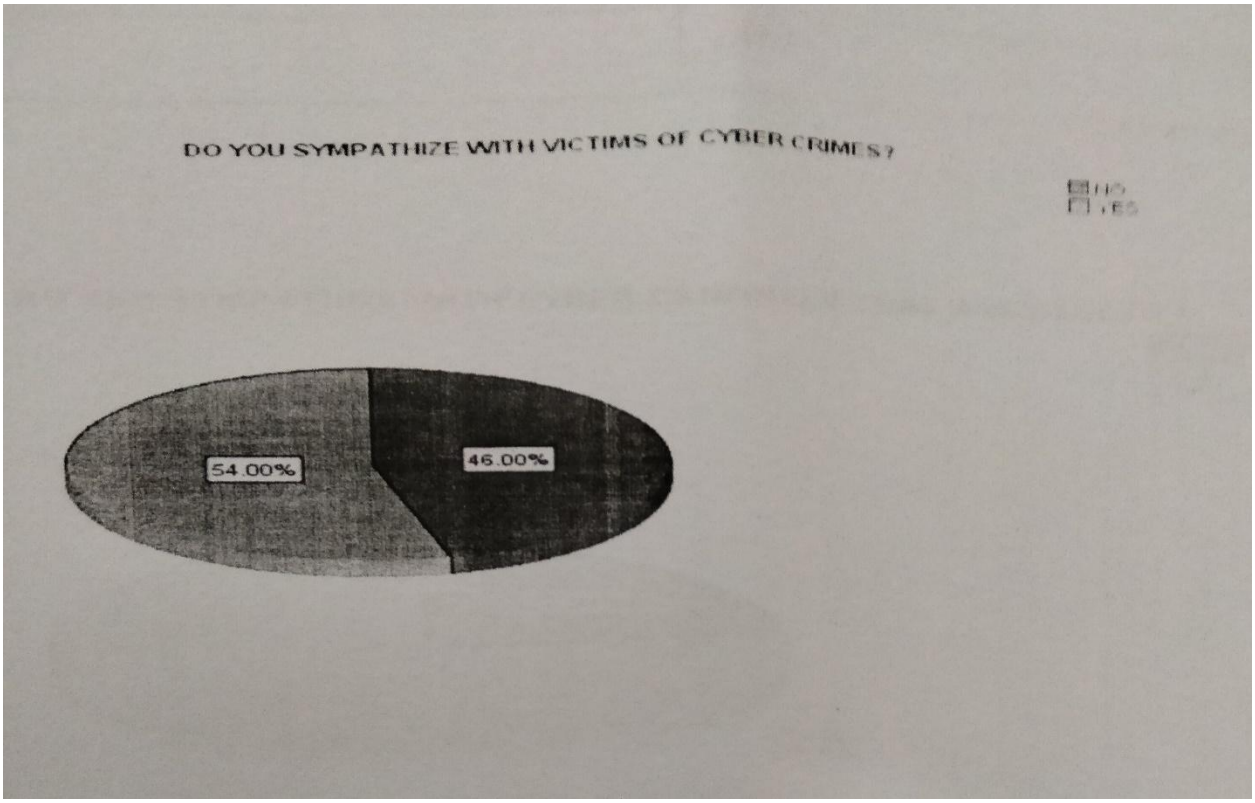
4.17 Research Question 18: Do you think EFCC can help stop cybercrime in Nigeria

This question was design to determine if respondents think EFCC Can stop cybercrime in Nigeria.

The result is shown in Table 4.18

DO YOU THINK EFCC CAN STOP CYBERCRIME IN	FREQUENCY	PERCENTAGE%

NIGERIA?		
YES	150	43.00%
NO	96	44.50%
UNDECIDED	54	12.50%
TOTAL	300	100

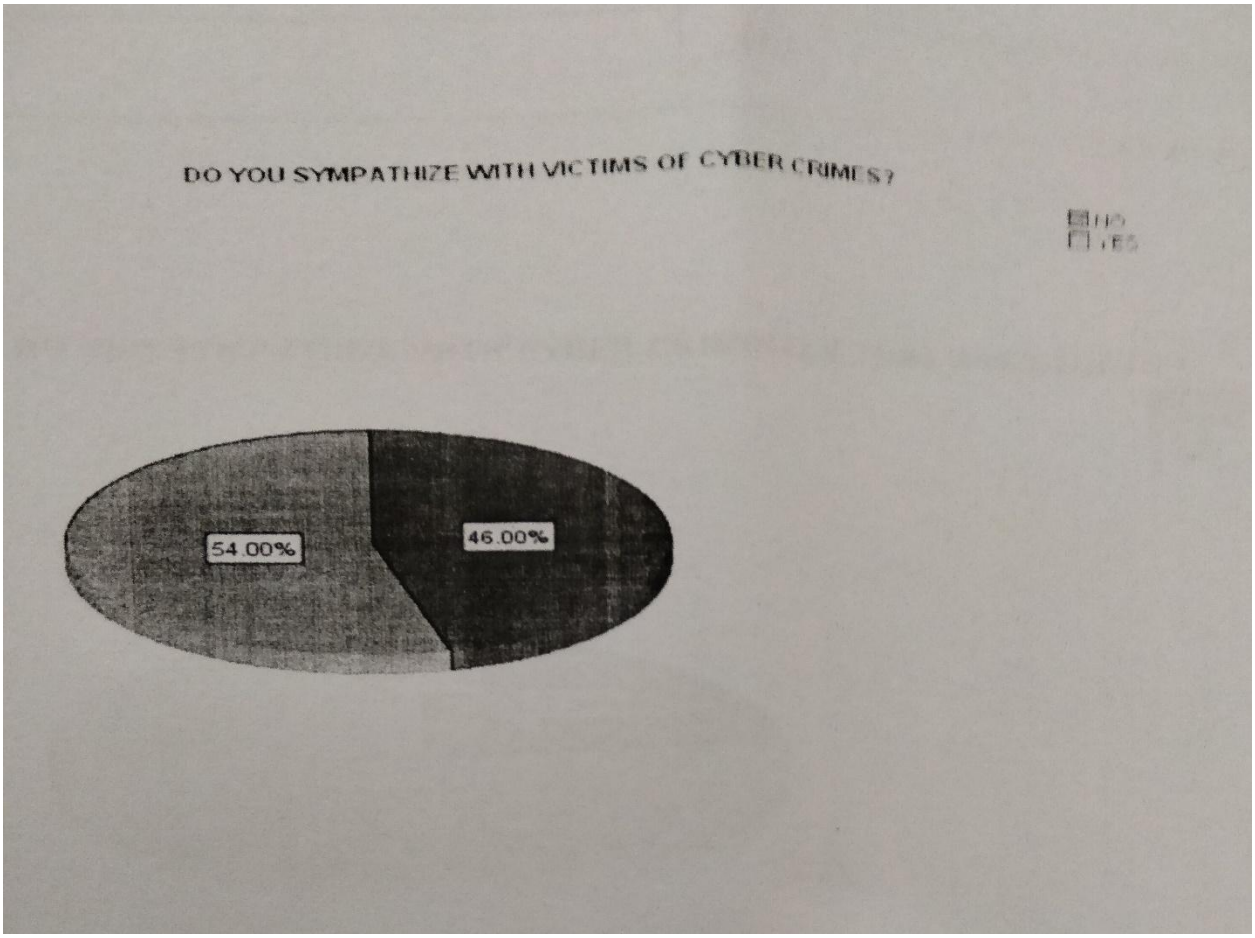


4.18 Research Question 19: Do you sympathize with victims of cybercrime?

This research question was design to determine if respondents feel sorry for cybercrime victims? The result is shown in Table 4.19

DO YOU SYMPATIZE WITH VICTIMS OF CYBERCRIME?	FREQUENCY	PERCENTAGE%

YES	208	54.00%
NO	92	46.00%
UNDECIDED	0	0.00%
TOTAL	300	100

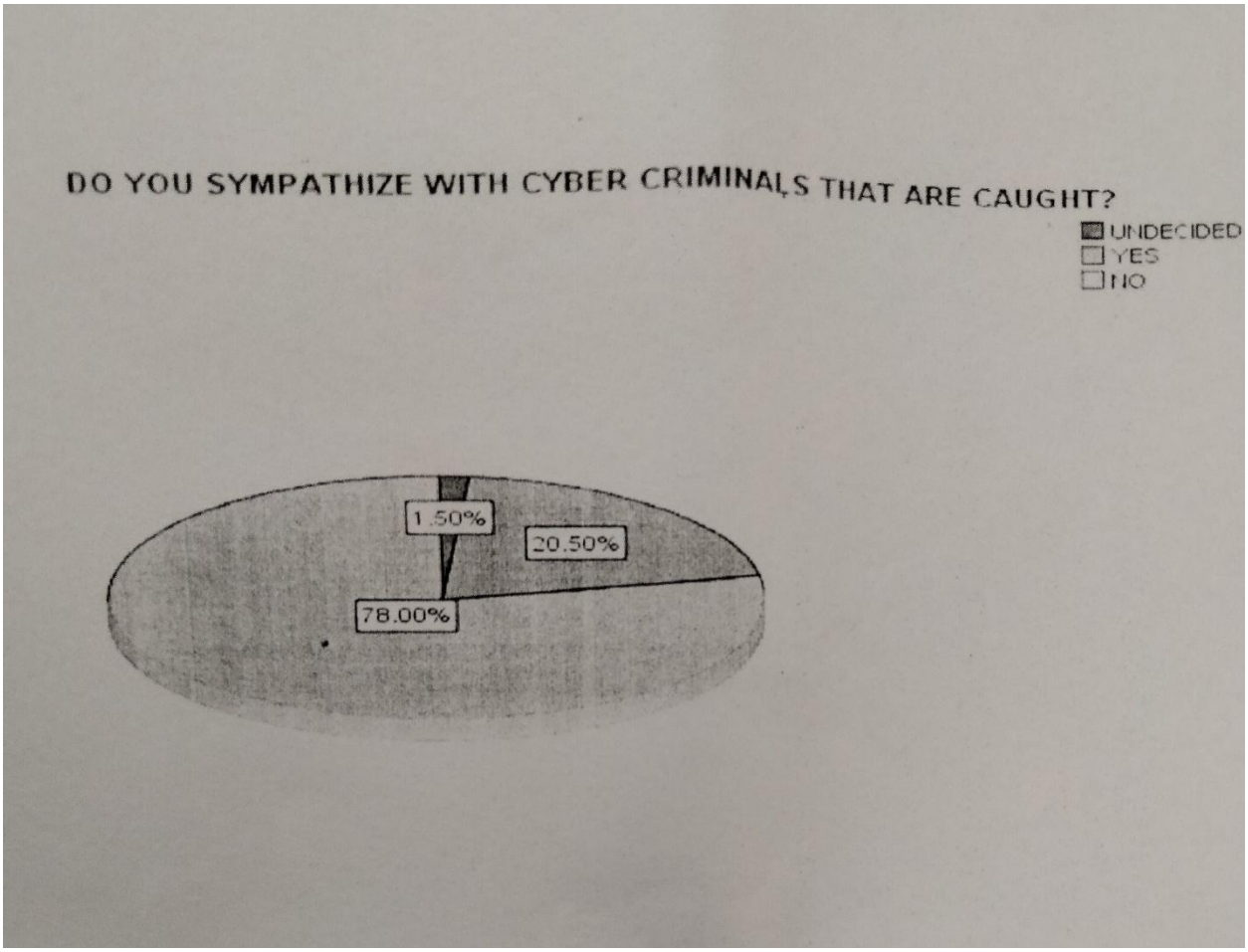


4.19 Research Question 20: Do you sympathize with cybercriminals if they are caught? This research question was design to determine if respondents feels sorry for cybercriminals who are eventually caught.

The result is shown in Table 4.20

DO YOU SYMPATHIZE WITH CYBERCRIMINALS WHEN THEY ARE CAUGHT	FREQUENCY	PERCENTAGE%

YES	46	20.50%
NO	250	78.00%
UNDECIDED	4	1.50%
TOTAL	300	100

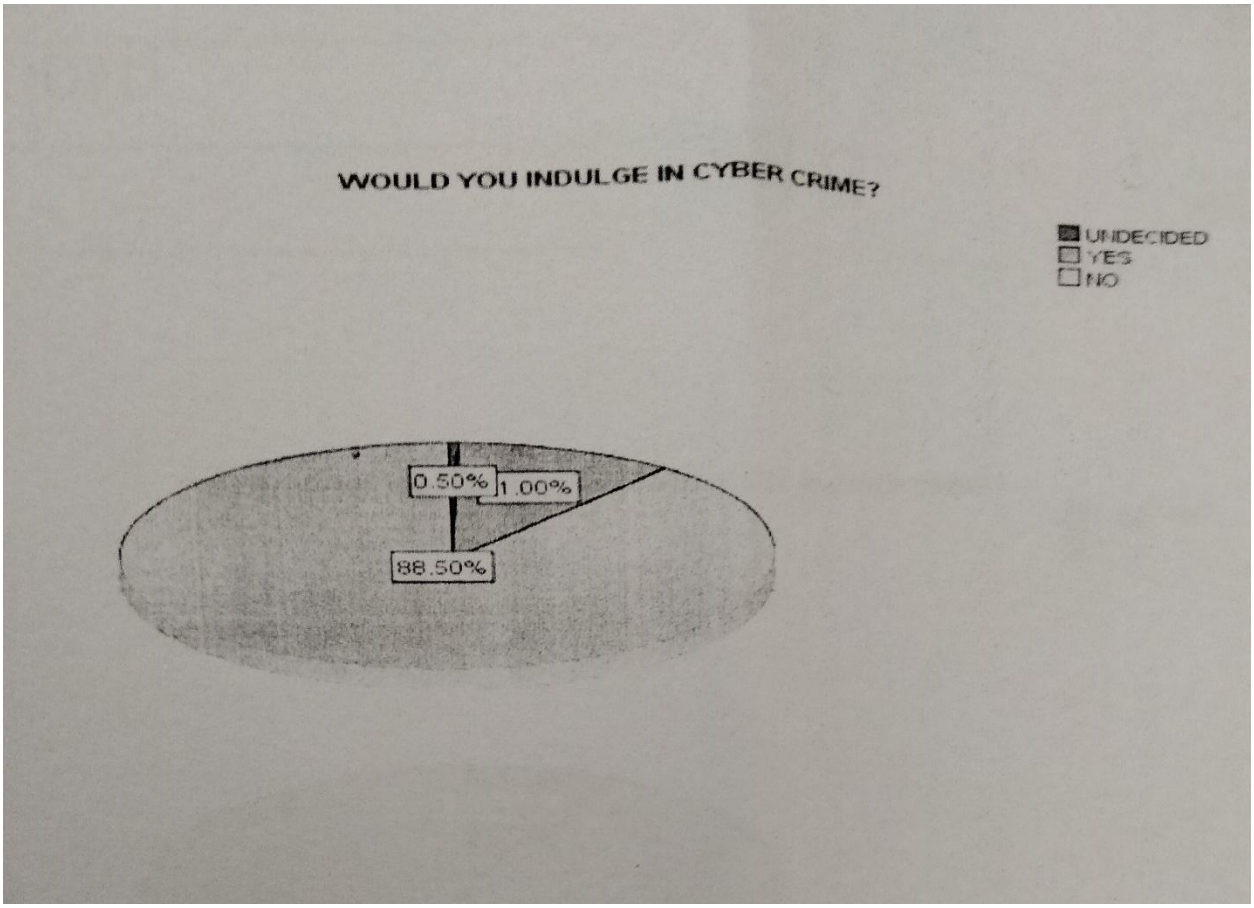


4.20 Research Question 21: Would you indulge in cybercrime?

This research question is used to determine if respondents view cybercrime as an area that would interest them. The result is shown in Table 4.21

WOULD YOU INDULGE IN CYBERCRIME?	FREQUENCY	PERCENTAGE%
YES	20	11.00%
NO	280	88.50%

UNDECIDED	1	0.50%
TOTAL	300	100



ANALYSIS

TABLE 4.1: SEX

Out of the 300 respondents that took the review, 59% were guys and 41% were females. Taking everything into account, greater part of the respondents were guys.

TABLE 4.2: AGE

From the diagram above, 36.50% of respondents were between the ages of 15-24, 25.5% were between the ages of 25-34 years while 23% are between the ages of 35-44 years. 10.50% percent of respondents were between the ages of 45 and 54, while the remaining 4.5 percent were 55 and older.

It is thusly most likely correct that larger part of the respondents were of the age between 15-24 years that is 85% of the absolute respondents.

TABLE 4.3: What Educational Level Are You Now?

The third examination question of the exploration instrument was utilized to decide the instructive degree of respondents. Since just 1.55% of the all out respondents are not taught by any stretch of the imagination. It hence shows that practically the entirety of our respondents were taught. This suits the examination Reason well.

TABLE 4.4: ARE YOU AWARE OF COMPUTERS

Respondents were asked to provide responses to Research Questions 4 and 5 regarding their awareness of and ownership of computers. Since the examination subject is connected with PC, it is vital to know the number of our respondents know PCs. According to the analysis, 99% of respondents stated that they are familiar with computers, and 79.44% of these respondents also stated that they actually owned computers. It is then protected to deduce that Greater part of individuals that answered have some familiarity with PCs and most really possessed PC sets.

TABLE 4.6: ARE YOU AWARE OF THE INTERNET

Research question 6 and 7 were utilized to decide the quantity of respondents that Is familiar with the web and furthermore utilize it. This will empower us to know the Level of the respondents that could have first ideal about the exploration subject, 98.49% said they knew about the web, a sum of 92% really utilized the web out of which 39.5% utilized the web at web bistro, 21.5% Said they utilized the web at home. 31% of respondents indicated that they use the internet both at home and in an internet cafes.

TABLE 4.8: DO YOU MAKE USE OF THE E-MAIL s

Research questions 8 was utilized to decide the rates of the respondents that have messages addresses from those that t really utilize the web while question 9 was utilized to decide the quantity of respondents that could have had experience with cybercriminal , who send trick sends to individuals E-email box. From the diagram, 87% said they have letter drops, 11.5% said they don't have email boxes while 1.50% were unsure.

In research question 9, 84.5% of the populace said they have gotten trick sends in their letter drops 12% said they don't get trick sends in their cases. 35% rate were uncertain about such sends.

TABLE 4:10 ARE YOU AWARE OF CYBERCRIMES

From the examination question, 89% said they knew about cybercrime while 10.5% said they were oblivious to cybercrime. Since an insignificant 0.5% said they were unsure, then, at that point, it will be protected to presume that greater part of our populace knew about cybercrime.

4.12: WHO DO YOU BLAME FOR CYBER CRIME AND ITS EFFECT.

From the above chart, 72.5% of our respondents said they accepted that the western world are liable for cybercrime and its impact. 23% said that Africans are at fault for it while 4.5% said they were uncertain on who is answerable for pattern. In this way since 145 respondents, that is 72.5% of the respondents said they accepted that cybercrime and its impact begun in the western world.

TABLE 4.13 DO YOU BELIEVE CYBER CRIME ORIGINATED FROM NIGERIA

48.50% accept that cybercrime didn't begin from Nigeria. 42% were certain that it began from Nigeria. The excess 9.59% were uncertain on the off chance that it really began From Nigeria or not. This is very As opposed to reaction for research question where most respondents were certain to the point that cybercrime and its belongings begun from the western world.

TABLE 4.14: D0 YOU THINK CYBER CRIME SHOULD BE AN ISSUE

OF MAJOR CONCERN IN NIGERIA.

51.5% believed that cybercrime should be taken up as a serious crime issue by the government of Nigeria. 43% 1eIt otherwise. The remaining 5.5% said they were unsure about how cybercrime should be treated in Nigeria. This was a close Call because a slight 8.5% was the different between those that that want Government to take up issues against cybercrimes and those that felt otherwise:

Though it is still significant but it is surprising that the difference is this small.

TABLE 4.15: WHAT ENHANCES CYBER CRIME IN NIGERIAN.

From the graph, it can be seen that 45.5% think that greed is responsible for the Increase in cybercrimes 33% think it is unemployment while 19.5% blame the Government for it. The remaining 2% said they were unsure what causes it in Nigeria. So majority of our respondents think that greed is the main reason why cybercrime continues to strive.

TABLE 4.16: IS THE GOVERNMENT DOING ENOUGH TO COMBAT CYBERCRIME IN NIGERIA.

67.5% of the total responses are of the opinion that government is not doing enough to stop cybercrime in Nigeria but 31.5% believed otherwise. Just 2 People, which is 1% of the population is undecided. So clearly, the majority of those that responded think that the government is not doing enough to punish and Stop cybercrime in Nigeria.

TABLE 4.17: WHAT NEEDS TO BE DONE TO STOP CYBERCRIME IN NIGERIANS.

Responses to research question 17 clearly Shows that 76.5%, more than half of the Total population believe that if government is able to create better living Conditions for Nigerians, most Nigerian cyber criminals would desist from

Involving in it. 15.5% believe otherwise, they believe that educating the youths would stop cybercrime.

A further 8% said that arresting all cybercriminals would stop cybercrime in Nigeria.

TABLE 4.18: DO YOU THINK THAT EFCC CAN HELP ERADICATE CYBERCRIME IN NIGERIA.

On the Issue of whether EFCC Can stop Cybercrime in Nigeria, the response's here was closely apart as 44.5% did not trust on the EFCC efficiency, a close 43% said that they believed that the EFCC was capable of eradicating cybercrime in Nigeria. 12.5% were neither of the opinion that EFCC was capable of stopping cybercrimes in Nigeria as they were undecided. However the Major believe here is that EFCC cannot stop cybercrimes in Nigeria.

TABLE 4.19: DO YOU SYMPATHIZE WITH VICTIMS OF CYBERCRIMES

54% said they sympathize with victims of cybercrimes while 46% believed they got what they deserved. It is therefore sate to conclude that majority of our Respondents sympathize with victims of cybercrime 78% said they sympathize with victims of cybercrimes while 20. believed they got what they deserved 5% of those that responded are undecided. Lt is therefore safe to conclude that Majority of our respondents do not sympathize with cyber criminals who are caught.

CHAPTER FIVE

Summary, Conclusion and Recommendations.

5.0 Summary.

Cybercrime makes adverse consequences and furthermore adverse consequences on the economy of a Country. However, its negative effects significantly outweigh its positive ones. In view of the examination directed cybercrime began in the western worrier but at the same time is exceptionally well known in Nigeria. Most Nigerians accepted that cybercrimes and It impacts is an incredible danger to the improvement of the country. Additionally, they believe that Nigerian law enforcement agencies lack the necessary computer forensics training to combat cybercrime. Many well-meaning Nigerians are uncomfortable with the numerous reports on cybercrime in the country.

These reports are harming the nobility of our country as a sovereign country. They are embarrassing and harmfully influencing our worldwide picture, our business, our psychological brain science and, surprisingly, our Youngsters. In any case, these reports focuses towards the way that Nigeria is working on a debilitated innovation stage and carefully uneducated climate that is in evolved nations, it is feasible to pressing need of master Arrangement since track all friendly messages that a specific web conventions (IP) is child d: All things considered. Sends from that can be followed back to it assuming perpetrating crime was utilized.

5.1 Conclusion

Because of the open idea of the web, cybercrimes is a pattern that has come to Remain, History bears us witness that no regulation made to battle customary wrongdoings have prevailed with regards to halting wrongdoing, consequently. No regulations will be ever adequate to stop wrongdoing completely. This likewise

applies to cybercrimes yet what we truly do know that when the fundamental things are set up, violations has been believed to tumble down to even an endurable and sensible level. Instead of attempting to stop cybercrime, Nigeria's response should focus on reducing it.

At the point when this is finished, then the battle against cybercrimes in Nigeria would have truly started.

5.2 Recommendations

From the examination on cybercrime, it was seen that its message to the economy of a country and even harmony and security is tremendous. Therefore, a holistic strategy is required to combat this crime in all its manifestations. It is consequently suggest that:

1. In Nigeria, cyber police who are specifically trained to deal with cybercrimes are needed. Moreover. A Central Computer Crime Response Wing should be established within the police force to advise the state and other investigating agencies on how to direct and coordinate computer crime investigations.

2. In addition, the establishment of a National Computer Crime Resource Centre—a body composed of experts and professionals to establish records rules, regulations, and standards, as well as the personnel of establishments and recognized organizations—is recommended. Firms, Businesses and so on. Moreover, Crime scene investigation commission ought to be laid out. Which will be liable for the preparation of criminology staff for Confirmation of every resident's.

3. T0 act as a security measure for people and corporate bodies. It is suggest that before anyone goes into any sort of monetary arrangements with anybody through the web he/she ought to utilize any of the web indexes like Google to check the character of the obscure individual via looking for their probable Past records, their sites and it appraisals to have some essential information about Such people and organizations. It ought to be noticed that this may not be sufficient to prevent an individual from been duped yet will just assist with discovering the lawfulness of a business manages a probable cybercriminal provided that such digital hoodlums records are posted onto the web by past casualties of such cybercriminal.

4. The Nigerian government ought to give work and businesses to young people since they are the ones that include more in cybercrimes

5. Over each of these, an extensive regulation to battle PC and digital related violations Ought to be declared to battle this "beast to a stop, this ought to be,

To additionally engage the EFCC.

REFERENCE

Eric Agwe-Mbarika Akutal, Isaac Monari Ong and Chanika Renee Jones (2011), Combating Cyber Crime in Sub-Sahara A frica:A Discourse on Law. Policy and Practice Journal of Peace. Gender and Development Studies Vol. 1(4) pp. 129-137.

Ewepu G, (2016) Nigeria loses NI27bn anually to cyber-crime NSA available

at:http://www.vanguardngr.com/2016/Nigeria-loses-n127bn- annually-cyber-crime-nsa/Retrieved Jun. 19. 2020.

G.O.0gunleye1, O.S. Adewale. B.K Alese and A.O. Ogunde (2011). A computer-based security framework for crime prevention in Nigeria. Journal of Nigeria Computer Society (NCS)

Hassan, A. B. Lass F. D. and Makinde J. (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology, vol.

VOL. 2(7), 626 – 631.

Lakshmi P. and Ishwarya M. (2015), Cyber Crime: Prevention & Detection, " International Journal of Advanced Research in Computer and Communication Engineering. vol. Vol. 4(3).

Longe O.B & Longe F.A (2005): The Nigerian Web Content: Combating the Pornographic Malaise Using Content Filters. Journal of Information Technologv Impact, Vol. 5, No. 2, pp.59-64, 2005

Longe. O.B. Chiemeke, S. C (2005) Cyber Crime and Criminality in Nigeria What Roles are Internet AcCess points in Playing? European Journal of Social Sciences - Volume 6, Number 4.

Longe, O.B.& Chiemeke, S.C. (2006): The Design and Implementation of An E-MaiEncryptor for Combating Internet Spam. Proceedings of the Ist International Conference of the International Institute of Mathematics and Computer Sciences. Pp 1 7. .Covenant University, Ota, Nigeria. Junc, 2006.

Maitanmi, O. Ogunlere. S. andAyinde S. (2013). Inipact of Cvber Crinnes on Nigerian Economy, The International Journal of Engineering and Science (JES, Vol. Vol 2(4), 45-51.

Okeshola F.B. and Adeta A.K. (013) The Nature. Causes and Consequence cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria American International Journal of Contemporary Research. Vol. 3(9), 98-114.

Omodunbi. B. A.. Odiase. P. O. Olanivan. . 0. M and Esan. A. 0. (2016). Cybercrimes in Nigeria: Analysis. Detection and Prevention. Journal of Engincering and Technology, Volume 1. Issue 1. September 2016 pp37-42.

Pereware Aghwotu Tiemo, Christina Uyoyou Charles-Iyoha (2008), Cybercafés And Cybcr Crime in Nigeria IGI Global.

Peter. G & Grace. D. (2001): Red Plags of Fraud. Trends and Issues in Crime and Criminal Justice. No. 200, Australian Institute of Criminology, Canbera

Available online at http://wwW.aic.gov. Au