UNIVERSITY FOR DEVELOPMENT STUDIES, TAMALE

ASSESSMENT OF THE PERCEPTIONS ON THE EFFECTS OF CYBERCRIME ON SENIOR HIGH STUDENTS IN TAMALE METROPOLIS: A CASE STUDY OF VITTING SENIOR HIGH SCHOOL

ABDUL-RAHIM MOHAMMED HARDI

2021

UNIVERSITY FOR DEVELOPMENT STUDIES

ASSESSMENT OF THE PERCEPTIONS ON THE EFFECTS OF CYBERCRIME ON SENIOR HIGH STUDENTS IN TAMALE METROPOLIS: A CASE STUDY OF VITTING SENIOR HIGH SCHOOL

BY

ABDUL-RAHIM MOHAMMED HARDI (B.A. Integrated Development Studies)

UDS/MDE/0016/18

THESIS SUBMITTED TO THE DEPARTMENT OF DEVELOPMENT EDUCATION STUDIES, FACULTY OF EDUCATION, UNIVERSITY FOR DEVELOPMENT STUDIES, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF PHILOSOPHY DEGREE IN DEVELOPMENT EDUCATION STUDIES

APRIL, 2021

DECLARATION

Student

I hereby declare that this thesis is the result of my own original work and that no part of it has been presented for another degree in this University or elsewhere. All references made to other studies have duly been acknowledged.

Candidate's Signature:……………...…………… Date:……………………..………

Name: Abdul-Rahim Mohammed Hardi

Supervisor

I hereby declare that the preparation and presentation of the thesis was supervised in accordance with the guidelines on supervision of thesis laid down by the University for Development Studies.

Principal Supervisor's Signature:………………………… Date:……………………..

Name: Dr. Ibrahim Mohammed Gunu

ABSTRACT

Background: Cybercrime refers to any crime or wrongdoing which is committed through the use of computer technology and internet to harm individuals and organizations. This crime cuts across all boarders and boundaries in the globe. It needs an inclusive approach by global cybersecurity organization and agencies to achieve success in the fight against cybercrime. This study aimed to assess cybercrime and its effects on students of vitting senior high school in the Tamale Metropolis of the Northern Region, Ghana. **Methods:** The study employed both qualitative and quantitative to gather data to achieve its objectives. Stratified and simple random sampling technique was used to select 329 respondents from various strata, form 1-3. Purposive sampling was also used to select key informants for interview. Data which was collected from questionnaire were analyzed using the Statistical Package for Social Science (SPSS). Qualitative content analysis was used to analyze the data that was gathered from the interview. **Results:** Data from the study revealed that majority of students 81.2% indicated that cybercrime is a very common practice among secondary school students which was confirmed by the key informants. The study deduced from both quantitative and qualitative data that vengeance or payback 73.6%, the quest for quick riches 58.7%, poor parenting 50.8%, fame 49.5%, poverty 48%, Internet literacy 46.5%, are the inspiring causes for students' involvement in cybercrime. **Conclusion:** Many of the respondents were knowledgeable in identifying the modus operandi of cybercrime practices and their source of knowledge were indicated as friends, internet, radio and television. The study revealed that going to jail, decrease ability to concentrate, poor academic performance, absenteeism and school dropout were some of the effects connected with cybercrime among students. Cybercrime and poor academic performances were linked where its practice led to decline in their academic performance.

ACKNOWLEDGEMENT

I will first of all express my gratitude to the Almighty Allah for granting me long life, energy, knowledge, resources among other things in pursuing my education.

My special acknowledgment equally goes to my supervisor Dr. Ibrahim Mohammed Gunu of University for Development Studies whose direction, and efforts aided the outcome of this study. His valuable contributions, encouragement, patience and assistance throughout the research will always be remembered. May Allah richly bless him.

My greatest appreciation goes to my parents; Mr. Abdul-Rahim Abdullai and Mrs Abiba Abdul-Rahim for ensuring that their son contributes to knowledge especially their contribution to my education and also my dear wife Mrs. Abubakari Hindu. My gratitude also goes to my dear brothers, Amin Abdul-Rahim, Abdul-Wahab Abdul-Rahim Maenu Abdul-Rahim and Baba Abdul-Rahim for their prayers, moral and financial support.

I am also indebted to Alhaji I.K. Antwi, former Librarian of University for Development Studies (UDS) who has been very helpful by way of encouragement.

I am also grateful to Mr. Edwin S. Thompson and the entire staff of University for Development Studies for their contribution and support.

I also thank family and friends whose great concern for my academic advancement is acknowledged.

DEDICATION

I dedicate this work to my family.

Table of Content

List of Tables

List of Figures

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background of the Study

The advent of Information and Communication Technology (ICT) for the past decades has brought massive improvement in all spheres of our endeavours. It is regarded as a major component in what is known as globalisation which connect the world with a much diversified ownership (Ige, 2008). The internet offers school children with many prospects such as easy access to information and also enables them to connect to the global world. These boost their cognitive and social development (Johnson, 2010). The degree of cybercrime has increased significantly in the last decade since the commencement of the internet and digital revolution in Ghana. In about two decades the internet has grown so large and become part and parcel of life of millions of people across the globe (Warner, 2011).

Accessibility and effective internet bandwidth in Senior High School (SHS) is considered as huge advantage for students as it will improve their level of comprehension, reading skills and improve their academic performance through browsing the World Wide Web. However, if this is left unsupervised it could lead students to internet crime (Singh and Bala, 2014). Uddin and Hassan (N. D.) stressed that unrestricted and constant use of cyberspace by young students has the ability to decrease their level of output in class. The undesirable connection between the academic performance of young students and excessive online internet usage is detrimental to their academic progress and could lead them to become cybercriminals. It takes away their precious time which could have been used to study for better grades. Barfi, Nyagorme and Yeboah (2018) reported that most students among the Senior High School in Ghana have ample understanding and awareness of cybercrime. They further indicated that SHS students are more familiar with the four main forms of cybercrime which are hacking, credit card fraud, software piracy and cyber identity theft. Igba, Igba and Nwambam (2018) stated that the internet has great effect on educational system and the advancement of every country. This has inspired people, establishments and other entities to establish cyber café which can give people easy access to current updates across the globe through the internet. This has given many opportunities to schools and other organizations to build their physical and intellectual properties to enable graduate to be useful to themselves and the society at large. However some people tend to use this innovation wrongly and abuse the rich resources the internet can offer leading to fraud or cybercrime.

Magele (2005) noted that the infiltration and diffusion of information and communication technologies (ICT) in Sub-Saharan Africa has fueled and injected new dimension of life style across all sectors of our daily transactions from education, entertainment, trades and businesses. These are ICT oriented businesses and services such as e-learning, e-banking, telemedicine, e-commerce, tele democracy. Magele (2005) further stressed that, this new level of development has come with a high cost and burden of new criminal activities known as cybercrime. Ige (2008) discovered that children under secondary school level use the internet to commit various acts of crimes. These crimes includes using other people credit cards and identities to steal money and buy goods online, send emails to foreign companies to steal dollars and pounds to the neglect of their studies.

School children also pornography and pictures to defraud people through the internet online dating sites. Basically, accessibility and use of internet and some other online resources in some parts of Sub-Saharan African countries largely depends on cybercafés. However, countries like Ghana, Cameroon and Nigeria have well established mobile internet facilities through satellite connections and other fiber optic cables which facilitate their online service provisions to their citizen (Abugri, 2011). Jones (2011) explains that the Africa sub region which was always describe as the “backward and dark” continent in the world has jumped into the ICT world with devastating consequences. This swift and fast rate of cybercrime in the African continent has been a very worrying situation and a call for concern by all stakeholders within the Sub-Sharan African. This situation even gets more worrisome by literature revelation that in the world top ten countries of high level of cybercrime dominance four of those countries come from Sub-Saharan African (Nigeria, Cameroon, Ghana and South Africa). The fight against cybercrime in Sub-Saharan African involves all stakeholders and should not be limited to law enforcement agencies (Jones, 2011).

In this era of ICT for development, it is not out-of-place to declare that cybercrime possesses some level of threat and can ruin the success of development emanating from ICT in Africa. Cyber fraud can damage information, other development infrastructure and also affect trust and confidence in electronic transactions and services (Salifu, 2008). The internet has become a necessary evil as Magele (2005) posits that “the internet has become a double-edged sword providing opportunities for individuals and organisations and also bringing with it an increased information security risk”. Strong internet band width and access to internet wireless connectivity coupled with personal computers, as well as smart mobile phones and other hand held electronic gadgets devices has enhanced business networks and valuable information online easily accessible. All these have resulted in effective and efficient service delivery in the global business environment. Undoubtedly, internet has come to change and simplify things in every aspect of our lives, from education, business, governance and health. However, it has come with some level of risks known as cybercrime. Over the past two decades, cybercrime has appeared as a noticeable field for survey and probe for criminologists and an increasing concern for civic and public policy.

Cybercrime generally refers to crimes committed through the use of computers and computer networks, but it also includes crimes that do not rely heavily on computers (Britz, 2008). Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission (Halder and Aishankar, 2011). Cybercrime, popularly known in Ghanaian parlance as “Sakawa” through the internet is common among the youths of school going age in Ghana. Ghana today is not like the late 1990s where only few minority rich classes had the privilege of owning a computer. The proliferation of e-waste has made it possible and cheap for most youth to purchase and own a second hand computer at very affordable price. Internet connectivity both wireless and cables has made internet usage very effective and useful as well as problematic among children of school going age from primary to junior high schools in Ghana (Warner 2011). Igba, Igba and Nwambam (2018) articulated that ICT which was seen as a tool for students to use to access information for their studies has now taken a different toll among students. ICT has now been used as tool to defraud people and use as a hiding place for students cyber fraudsters.

1.2 Problem Statement

The Centre for Strategic and International Studies (CSIS, 2013) in a survey indicated that cybercrime is considerably affecting global business transactions. It leads to loss of revenue in the global market economy ranging from the manipulation of the stock market, loss of trust for online transactions, intellectual property loss and other important and sensitive business information. Cybercrime affects government spending which has effects on the disbursement of national resources for effective productivity in the country. CSIS further indicated that globally, the world losses a tune of $400 billion annually through cybercrime and this amount to about 1.2% of global GDP. International Telecommunications Union (ITU) revealed that the growth and tendencies of cybercrime is on the rise as cybercriminals consistently adopt new technological approaches to advance their criminal online activities. These approaches appear more profitable to these cybercriminals. United States alone incur $52.5 million and $67 million financial losses in 2006 and 2007 respectively through cybercrime (ITU, 2008). A report release by the FBI National Press Office in Washington, D.C on the internet complaints indicated that a total of 301, 580 complaints of suspected criminal internet activities were received in 2017 by the Internet Crime Complaint Center. Losses of $1.4 billion were recorded and the top crime complain by targets were non-payment/non-delivery, personal data breach and phishing (Internet Crime Complaint Center (IC3), 2018). The Attorney General's Department of Australia (AGDoA) revealed that $2 billion are lost annually by the state. This cost is described by AGDoA as non-governmental cost which means every Australian citizen including school children are affected by the actions and operations of cybercriminals (AGDoA, 2013).

The introduction of ICTs has played a very significant role at various levels in a young emerging economy like Ghana. This has manifested with the introduction of interventions such as, e-Justice system, the paperless port system, the construction of National Data Center (NDC), deployment of national ICT infrastructures, and the laptop per child policy in our schools show that Ghanaians have fully accepted and embraced ICT cyber-based society. National Development Planning Commission (NDPC, 2012) have indicated that the introduction of ICTs in our national development agenda have yielded positive results. ICT contribution to the Gross Domestic Product has increased from 2.3 percent in 2009 to 10.5 percent in 2011 and also created 3,500 additional jobs in 2011 compared to 3,050 in 2010 (NDPC, 2012). Despite the success Ghana has achieved through ICT, it is not out of order to say that cybercrime and other related internet fraud are in the widespread. Reports in dailies give credence to the fact that this menace is on the increase. In April 15, 2013 edition of the Daily Graphic (a popular daily newspaper in Ghana) reported that Ghana has been placed seventh out of ten countries in the world and second within the Sub Sahara Africa (SSA) in the cyber fraud is worrying. What is more worrying about this phenomenon is the fact that a lot of young children among school going age are engaged in these crimes (Daily Graphic, 2013). Kwablah (2009) stressed that Ghana has been earmarked as the second most commonly blocked location by U.S e-commerce sites because online traders are skeptical of fake orders from internet scammers. This has made it difficult for most Ghanaian business men to gain trust and the credibility in marketing our local product which could earn the country some foreign exchange to improve our educational system. It also scares away foreign investor who could genuinely come to Ghana to invest in order to create employment and income for our young graduates.

In this digital modern era where people are moving to paperless society, most young children of school going age spend most of their time browsing the internet via computers and other personal electronic gadgets. These provide quick access and means of communicating across the World Wide Web. However, easy access to the cyber space and internet, when left unchecked, could affect and destroy the minds of these young future leaders in Ghana. Especially, if they keep getting huge money, cloths, cars, laptops and other valuable properties through cybercrime (Sakawa) and other related internet fraud. The future generation may turn down schooling and opt to concentrate on making more money through internet fraud (Sakawa). This study therefore seeks to assess cybercrime and its effects on educational performance among students of Vitting Senior High School (SHS) in Tamale Metropolis of Ghana.

1.3 Main Research Question

What are the perceptions of cybercrime and its effects on academic performance among students of Vitting Senior High School in the Tamale Metropolis of the Northern Region, Ghana?.

1.3.1 Specific Research Questions

1. What is the knowledge level of students on cybercrime in Vitting Senior High School?
2. What are the factors that influence students into cybercrime in Vitting Senior High School?
3. What are the effects of cybercrime on academic performance of students in Vitting Senior High School?

1.4.1 General Objective

The main objective of the study is to assess cybercrime and effects on academic performance among students of Vitting Senior High School in the Tamale Metropolis of the Northern Region of Ghana.

1.5.1 Specific Objectives

Specifically the study is to:

1. To assess the knowledge level of students on cybercrime in Vitting Senior High School.
2. To identify factors that influence students into cybercrime in Vitting Senior High School.
3. To assess the effects of cybercrime on academic performance of students in Vitting Senior High School.

1.6 Significance of the Study

The revolution of ICTs has created a myriad of opportunities to mankind but cybercriminals are frustrating the significance of this invention. Criminals have deviced varied ways and means to defraud innocent people through cybercrime and other internet fraud. This and many others have necessitated this study to equip readers with a better understanding and also create awareness about the numerous strategies adopted by cybercriminals in scamming people. It will also bring to bear on some means and ways of combating cybercrime and other related online/internet fraud.

The study also intends to add to the literature on the prevalence of cybercrime among SHS students and its effects on their academic progress. It also seeks to give estimates on the knowledge on cybercrime and its effects, on the individual and the country at large. Such information will serve as an important measure and provide focus for various intervention and prevention programmes, especially those directed towards young school children. The results of the research could also be used as a decision making tool or input for policy makers, especially Ghana Education Service (GES).

1.7 Scope of the Study

The study was carried out at the Vitting SHS of Tamale Metropolis. The subjects for this study will be students from SHS 1-3 both boarding and day students.

1.8 Limitation of the Study

Every study has limits or restrictions which are unavoidable. First and foremost, the number one limitation was time restriction. The time limit for the administering of the questionnaires was short. The subject of cybercrime is complex, sensitive, criminal and confidential and people involve feel uneasy to talk about it. The probability of respondents volunteering inaccurate responses to the questions could be very high.

1.9 Organisation of Chapters

This report has been organised into six chapters. Chapter one contains the introduction which will provide an overview of the study. It covers background of the study, statement of the problem, purpose of the study, objectives, research questions, scope of the study, theoretical framework, and significance of the study and organisation of the chapters. The second chapter reviews relevant literature which provides information on the context for the research. It features the following sub-themes, definitions of cybercrime, cybercrime in Ghana, cybercrime legislations in Ghana, causes of cybercrime, forms of cybercrime and cybercrime and educational progress.

Chapter three explains the methodology adopted for the study. These consist of the study area, study design, study population, sample size, sampling procedures, sources of data, study variables, instruments for data collection, data collection procedure, data analysis and presentation of results, training and pre-testing, quality control, limitations of the study, dissemination of findings, ethical issues involved and how it is addressed. Chapter four focuses on presentation and analysis of results from data to be collected. The fifth chapter concentrates on discussion of findings and chapter six which is the last chapter look at the summary, conclusion and recommendation aspect of this study.

1.10 Conclusion

This chapter encompasses the introduction which provides an overview of the study. It also covers background of the study, statement of the problem, purpose of the study, objectives, research questions, scope of the study, theoretical framework, and significance of the study and organisation of the chapters.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviewed evidence involving cybercrime and its effects on academic performance among young children of school going age from related several sources which include online journal articles, textbooks, newspapers, theses and dissertations. According to Creswell (2014) literature review communicate with researcher and the reader the findings of other research which are interrelated to the one being understudy. It narrates a study to the bigger society by comparing and filling in the gaps created in previous related subjects been understudy. In light of these, the literature was reviewed along the following sub-themes: theoretical framework; definitions of cybercrime; cybercrime in Ghana and beyond (globally and Africa); cybercrime in African Continent; cybercrime in the World; forms of cybercrime; cybercrime legislations in Ghana; causes of cybercrime; and effects of cybercrime.

2.2 Theoretical Framework

This deals with the theory which strengthens the study. Theoretical framework describes the theory that explains why the research problem under study exists. It helps the researcher to explain the research questions or hypotheses. Theoretical framework also gives explanation to causes and effects and also helps the researcher to come out with the types of research questions that need to be addressed (Clark and Creswell, 2011). Again, this also serves as modules that guide the organisation and data collection procedures in the research. Various theoretical concepts are adopted by researchers in dealing with crime. One of these technologies adopted for this study will include:

2.3 Social Strain Theory (SST)

This study adopted Merton's strain theory to explain cybercrime activities of the senior high school students in Tamale Metropolis. Merton (1938) is a pioneer of this major theory to offer better explanation and understanding on criminology. Merton (1938) contends that everybody in a society is encouraged to struggle for opportunities in terms of monetary success. However, lower class people are often sidelined and denied towards the attainment of such goals through genuine means. When such a situation occurs such individuals are unable to provide their families with school fees, skill, businesses and other basic needs necessary for their future success. Consequently, such lower class people develop a strain. This strain disconnects them from achieving their goals through legitimate means. Merton expanded Durkheim's anomie theory to give clarity to a diversity of deviant conducts in our societies (Hilbert, 1989). Hilbert (1989) refers to strain or anomie "as the imbalance between culturally defined goals and socially or institutionally presented means for realising these goals". This implies that some individuals are most likely not to attain these culturally approved goals through the approved institutional means, hence they veer to unauthorised means to obtain these cultural goals by other ways. To some individuals there is structural strain between the goals and means of society. Merton acknowledged five answers to these problems of deviance. These deviances are: Conformity, Innovation, Ritualism, Retreatism and Rebellion.

Conformity; this conforms with and takes recognition of the cultural goals and means of attaining those goals. Innovation; this kind of deviance chases goals whiles rejecting legitimate means rather than adopting illegal/ illegitimate means. Ritualism; here cultural goals are rejected but rather accept the legitimate means of achieving goals. Retreatism; this however, refuses or rejects both the cultural goals and the traditional means of achieving those goals. Rebellion; in this case people abandon both goals and means but aggressively tries to swap both goals and means with different social structures (Merton, 1968). Among the five deviance adaptations, four of them deviate from culturally goals or socially and institutionally accepted means of attaining success in the society. For the purposes of this study, the emphasis would be on the Innovators.

The innovator could possibly accept the socially approved means to achieving success. However, limited possible means of reaching such success could deviate them from following the right channel. He may therefore decide to innovate his own possible means to achieve institutionally goals through other unlawful means, for example armed robbery, drug dealers, prostitutes and cybercrime (sakawa). Merton's strain theory pointed at those who are involved in criminal activities such as cheating and other dishonest ways of accomplishing success. However, in Ghana there is no specific law that limits people in terms of wealth acquisition. Abotchie (2012) claims that to the innovators, whilst the urban culture stresses on material accomplishment, the truth remain that social institutions in our societies put limits to the approved means of accomplishing success. Abotchie (2012) further stress that as a results of the extreme composition and struggle for success in our urban communities, Merton's innovation is seen as the obvious choice to adopt for survival.

2.4 Differential Association Theory (DAT)

Another well-known established theory which offers a clear explanation to criminal behaviour is Edwin Sutherland's Differential Association which was developed in 1939.

This is a scholarly learning theory of criminology and deviance in our societies. Regoli and Hewitt (1997:181) stressed that this theory has continued to be extremely significant in the field of modern criminology regarding how people reflect on crime as differential association. According to Sutherland (1939) "criminal behaviour is learned in the same way as law-abiding values are learned, and that, this learning activity is accomplished in interactions with others through a process of communication within intimate groups. He further argues that, just as one can be socialised into good behaviour, so also can one be socialised into bad behaviour". The theory sustained its relevance because of its comprehensive ability to explain all types of criminal action, from juvenile delinquency to white collar crime.

The theory of differential association consists of nine principles:

1. All criminal behaviour is learned; it is not hereditary. This implies a person who is not already educated or learned criminal act cannot develop such acts.
2. Criminal behaviour is learned through interactions with others via a process of communication. This communication could be verbal and non-verbal.
3. The learning occurs within the intimate groups and relationships: This means that peer or family groups and relations are the most likely sources of initiation into deviance and criminal beliefs and actions. By this Sutherland implies that, impersonal agencies of communication such as picture shows movies, social media, newspapers play relatively unimportant part in the creation of criminal behaviour.

4. The process of learning criminal behaviour may include learning about techniques to carry out the behaviour as well as the motives and justifications that would defend criminal activity and attitudes necessary to orient an individual towards such activity.
5. The direction of motives and drives towards criminal behaviour is learned through the interpretation of legal codes in one's geographical area as favourable or unfavourable.
6. When the numbers of favourable interpretations that support violating the law outweigh the unfavourable interpretations that do not, an individual will choose to become a criminal. This is the central belief of differential association theory. It reinforces the belief that the definitions favourable to the violation of law can be learned from both criminal and non-criminal people.
7. All differential associations are not equal. They can vary in frequency, intensity, priority, and duration.
8. The process of learning criminal behaviours through interactions with others relies on the same mechanisms that are used in learning about any other behaviour. This means that, the methods for learning criminal behaviour are the same as those for law abiding values and other socially relevant skills. The suggestion is that, in as much as the content of what is learned is different, the process giving rise to criminal behaviour is the same as any other law-abiding behaviour.
9. Criminal and non-criminal behaviours all express generalised needs and values. In other words, the objectives and goals of criminals and non-criminals are generally the same. For instance most cybercriminals defraud people in order to make

money. Likewise genuine people work with the financial value in mind. What differentiates them is their approach in achieving this same goal.

Differential association theory has played a very significant role in providing explanations to criminal behaviours in the field of criminology. However, the theory has received some critiques.

Sutherland and Cressey (1978) posit that high crime rate is due to differential social organisation. In places where crime rates are high, interactions with other people could lead a decent child to learn and gain unacceptable behaviours within the area. The theory has been criticised by some intellectuals who claim it is a flawed as it fails to take into account of people who commit crimes out of their free will. People are self-regulated, independently motivated beings. Sutherland was also criticised for failing to consider people who indulge in wrongdoing due to their personal characteristics like aggressiveness. However, the theory has been instrumentals in clarifying how lawbreakers acquire their lawless behaviours.

2.5 Definition of Cybercrime

The complex nature of the term cybercrime has made it very difficult in giving a precise definition. Smith, Grabosky and Urbas (2004) indicated that it is often complicated in getting a unique and consistent definition of cybercrime. This has resulted in multiplicity of terms such as computer crime, computer-related crime, digital crime, information technology crime, internet crime and virtual crime. Alkaabi (2010) articulated that, traditionally, the term cybercrime referred to crimes over networks, especially the internet but the term has increasingly become a general term or replacement for computer crime. Kamal, Chowdhury, Haque, Chowdhury, & Islam (2012) articulated that presently crimes which are committed in the cyber world are not different in this present world. Crimes committed in the cyber world are so complex in nature and its coverage is very wide and massive. There is no precise definition of the term cybercrime. This is because different institutions, departments, organisation and agencies have given different definitions in accordance to their situation and place. Cybercrime is a split word which can be better understood by understanding the split meaning of cyber and crime. According to Anah, Funmi, & Makinde (2012) the word "Cyber" comes as a prefix which is often used to define a new knowledge or idea associated with computers and the internet and "Crime" any act which is considered as wrongdoing or illegal and punishable by law.

Parker was one of the pioneering scholars to write about computer crime. He was adjudged the best scholar on computer security in the United State. Parker uses the term computer abuse to mean computer crime in order to escape having to distinguish between what is crime and what is not. Parker (1980) define his computer abuse as "any international act in which one or more victims suffered or could have suffered a loss, and one or more perpetrators made or could have made a profit." United Nations (UN) Tenth Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined as:

a. Cybercrime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

b. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

UN further acknowledged that these definitions are complicated by the fact that an act may be illegal in one nation but not in another. Cybercrimes are defined as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, emails, notice boards and groups) and mobile phones” (Hassan, Lass, & Makinde, 2012). Snail (2009) further explains that cybercrime can be defined as any criminal activity that involves a computer. This can be divided into two categories; crimes that can only be committed using a computer which were previously not possible before the dawn of the computer. Examples hacking, sniffing and the production and dissemination of viruses. Secondly, crimes that have been in existence for centuries but now committed within the cyber environment such as fraud, possession and distribution of pornographic materials. The United Kingdom (UK) Association of Chief Police Officers (ACPO) has defined e-crime as the “use of networked computers, telephony or internet technology to commit or facilitate the commission of crime.” Wall (2007) stated that the term cybercrime “has a greater meaning if we construct it in terms of transformation of criminal or harmful behaviour by networked technology, rather than simply the behaviour itself” he therefore interprets the term cybercrime broadly to refer to “criminal or harmful activities that involves the acquisition or manipulation of information for gain”. Olayemi (2014) articulated that cybercrime might rationally comprise of a wide collection of criminal records or offences and it would rather seem like researchers, academicians and law implementation authorities are more free and relaxed to labelling several factors constituting cybercrime rather than trying to define it.

2.6 Worldwide

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.

2.7 African Continent

The infiltration and acceptance of Information and Communication Technologies (ICTs) in the 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” 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 is 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 3rd 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 the adolescents representing 85%. Related crimes comprise child pornography, hacking sites to get access to credit cards and downloading films for sale. The monetary connected crimes have been termed as “Sakawa” in Ghana.

2.8 Cybercrime in Ghana

Internet usage has witnessed a significant upsurge since the improvement of the telecommunication industry in the 1990s. For instance, Ghana had 43 internet user per one thousand people in the year 2008 compared to 1 internet user in 1999. Again, people who own personal computers (PC) also doubled to 52 people per one thousand people between 1999 and 2005 (ITU, 2008). This development has its accompanying negative effects on the country. Ghana is often seen as a beacon of Africa, had its good name tarnished when it was reported that, Ghana has gained the unsavory distinction along with Anglophone African neighbours Nigeria and Cameroon as one of the top ten cybercrime generating states worldwide (Warner, 2011). Statistics from the Cybercrime Unit of the Criminal Investigations Department (CID) at Ghana National Cyber Security Center (GNCSC) by the Finance minister shows that, Ghana lost about US$25.8 million in 2016. This figure increased to US$ 69 in 2017. An assessment further indicates that as at August 2019, the country has lost US$97 million due to Cybercrime. This suggests that cybercrime is increasing in Ghana.

Cybercrime is a relatively new phenomenon in Ghana. According to Warner (2011) cyber-fraud came to rise in Ghana between 1999 and 2000. During this period, electronically based crimes were primarily related to credit card fraud, which was initially facilitated by bellhops at international hotel chains who would share Western visitors' credit card information with scammers. In these instances, Ghanaians would steal the numbers of Western credit cards, purchase goods from the internet, and have them shipped to Ghana. However, since approximately 2004, credit card purchases over the internet have dropped; instead, newer forms of internet fraud have begun to take shape. International Telecommunication Union disclosed that 1,297,000 Ghanaians uses internet which represents 5.3% of Ghana's population as at 2010. The internet plays a very significant role in the growth of business and the national economy. Improved Internet has its accompanying negative consequences. Duah and Kwabena (2015) explain that "Sakawa" is a Hausa word which entails the root 'saka-' meaning [to put it in] and 'wa' (a simultaneously past and plural affix). Joining, these two literally mean 'to [have] put something in. 'Sakawa' is an invention by youth scammers from underprivileged communities in Accra such as Nima, Mamobi and Lagos Town. Sakawa is an "azaa" (deceitful) act where cyber scammers believed to have involved some rituals and cultism with the intention to oblige their victims to comply with their request. These so-called rituals encompasses taking an oath not to reveal 'sakawa' secrets and to completely accept by 'sakawa' rules; inflicting wounds that never heals; sleeping in coffins for specified days at cemeteries (maximum being a week) drinking human blood to mention but few. They further disclosed that the popular scam in Ghana include gold, diamond, lottery and some abandoned money that the client can help recover. The scammers orchestrates a well diplomatic ideas with better explanations supported with fake documents coming from genuine sources such as the Office of the President, Attorney General's Department and reputable banks (Duah and Kwabena, 2015).

Historically, scamming and other computer related crimes in Ghana is more like benevolent services which school children use to write letters to foreign pals to asked for petty gift like pens, books, T-shirts and other items via postal system. Cybercrime gained its root from this practice in Ghana. Scammers drew most of their inspiration and tactics from these foreign pen pal relationships to exploit Westerners either through social networking websites like Twitter, Facebook, and Tango or through internet dating sites like porn.com mylove.com to target mainly Westerners for economic benefits. These practices have come to substitute the contemporary day internet fraud popularly known in Ghana as ‘Sakawa’ (Burrell, 2008). In Ghana 90% young males below the ages of 30 are involved cybercrime (Warner, 2011). Abugri (2011) concluded that many of them reside within the Central Business District and capital cities like Accra, Takoradi and Kumasi, where they can have easy access to internet services. Warner (2011) studies of cybercrime in Ghana have discovered three main sources that sakawa or cyber fraudsters normally implore to dupe victims. These include, identity fraud, scammers will disguise themselves to be people they are not to defraud Westerners who are not fortunate to fall prey. This is mostly done through Facebook and other internet site designated for dating such as Match.com, or eHarmony.com. After winning the trust of victims through chatting and other means of contacts, scammers begin requesting for business and financial information and passwords of their supposed love. This is termed as romance scam. Fake gold dealers, Ghanaian Sakawa mostly boys make contact with some white men online and offer them deals in gold investment. As the deal unfolds they invite them to come to the country to assess some fake gold mines. They arrange for their pick up at the airport show them real gold to affirm the deal and later run with their invested money in the deal. The third is the estate fraud. The estate deals mostly target fellow Ghanaians living in abroad (burgers). Scammers pretend to be estate developer by advertising their construction companies which are fake via the internet. Some of these Ghanaians in the diaspora express interest to buy such properties. Ghanaian “burgers” that fall victims are made to pay moneys for cost of plots, building materials and other expenses. After milking huge sums of money from these "burgers" such dubious companies are closed down and the scammers then disappear (Warner, 2011).

2.9 Forms of Cybercrime

Effective internet bandwidth couple with ICT has brought about massive growth of cybercrime globally. Every online tool such as computers, android phones and tablets have been connected to the internet. Criminals attacked individuals, corporate institutions and governments through the World Wide Web to make money. This crime is witnessing increases every time. Cybercrime is largely divided into two broad forms. These are crimes that target networks or devices (viruses, malware and DoS attacks) and crimes using devices to commit criminal activities (phishing e-mails, cyberstalking and identity theft). Cybercrime is been characterised by three main groups; namely individual, property and government (Types of Cybercrime, 2018). Property scammers steal people's bank accounts details and credit card particulars to gain access to their funds. They could use such information to buy goods online. They also use malicious software to access web pages containing classified information. The individual scammers involve one person dispersing malicious or illegal information online. Government cybercrime is very serious crime among all the categories. It is other words known as cyber terrorism. These criminals are usually perpetrated by extremist or opponents. These comprise of hacking government websites, military websites or distributing propaganda stuff (Types of Cybercrime, 2018).

- **Identity Theft**

Modern business offer clients' opportunity to transact business remotely and payments are done via online for good services purchase. However, over reliance on such transactions without putting appropriate mechanisms will also create an opportunity for fraud. Some of these online clients are total strangers to each other. They got to know each other online. The system often connects sellers and buyers to a links of data with specific account or credit details. Identity theft consists of obtaining sufficient information about different individual and forged the link which enables the thief to obtain the goods and services while accrediting the burden to another person's account. Unidentified or anonymous data-based transactions have characterised the credit card payment system for decades. However, the over dependence on data for payments have also breed new prospects for fraud (Anderson, Durbin & Salinger, 2008).

Merriam-Webster online dictionary define identity theft as the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit. Daniel (2015) explained that there are diverse forms of systems which are used by identity fraud offenders to defraud victims. Some of these techniques include technical and social engineering tactics. These ranged from technical and social engineering strategies. The social engineering happens when somebody is either in person, in a phone or computer, implores tactics to deceive different person to reveal sensitive information. Normally, the social engineer has level of knowledge about their victims and motivates victims to trust such criminals are honest and clean to deal with and finally fall prey to scammers. In the same manner, cybercriminal who are ICT compliant may trick the internet to redirect people e-mails to a different without their permission. They could do this by discovery user's passwords through hacking, recovering individual data through social media, or sending phishing emails.

- **Malware**

According to Merriam-Webster online dictionary malware is software designed to interfere with a computer's normal functioning. Cybercriminals inject viruses, worms Trojan horse, adware and spyware over the cyberspace to attack individuals, corporate and even government websites to collect vital information for them. Malware is computer code designed with malicious intentions. Occasionally, malware is categorically used to attack government or company websites to collect protected information to interrupt their process and procedures to their advantage. However, malware can also be launched to attack persons in order to gain access to their personal details such as personal identification numbers, bank details, credit card numbers, and passwords to defraud them (tapestrynetworks.com, 2015). Availability of bandwidth has also increased the manufacturing of malicious computer software for profit.

- **Ransomware**

The Cybersecurity and Infrastructure Security Agency (CISA) define ransomware as "type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid". They have detected that this form of attack is in the rise globally. It is reported that 181.5 million ransomware attacks cases were recorded between January to June in 2018 which represents 229% rise within the same period in 2017. Ransomware attacks are classically design using a Trojan that is camouflaged as a genuine file which deceived users into copying, downloading or opening when it drops as an e-mail attachment. Security Engineering Research Team (SERT, 2016) threat report concluded that 88% of ransomware attacks are aimed at healthcare providers such as hospitals and other health organisations. Scammers believed that such schemes are susceptible. They often pay cybercriminals their ransom to avoiding risking precious innocent lifes.

- **Credit Card Fraud**

Modern technology has made businesses to transact and transfer money electronically. This has gain massive recognition and patronage by general populations. However, cybercriminal are devising new innovative ways to steal people's money which poses a bigger challenge to the digital economy. Schmalleger and Pittaro (2009) explained that Credit Card Fraud is a kind of scam where criminals uses someone else credit card to make transactions without the knowledge of the original owner that his/her card is being used. This is an illegal use of different person's credit card or bank details for profit through fraud and impersonation. Eurobarometer carried out a study in 2013. The study covered over 27000 participants in all member states. The results have shown that 76% of the respondents agree that there is very high danger of becoming credit card/banking online fraud victimised. This act of criminality is increasing every year. Cybercriminals put fears in individuals and organisations to make good use of the cyberspace in order to enjoy the benefits of the internet and other online transactions.

According to the Nilson (2019), worldwide losses from card fraud rose to $27.85 billion in 2018, an upsurge of 16.2% from $23.97 billion in 2017. Out of the global figure 33.99% represents US losses and the figure is expected to reach $35.67 in 2023**.** Graphic online states that there is numerous form of credit card fraud which keeps on changing frequently with changes in technology. It identifies only two main categories as follows:

Card-Not-Present (CNP) **frauds:** This, the most common kind of fraud, occurs when the cardholder's information is stolen and used illegally without the physical presence of the card. This kind of fraud usually occurs online, and may be the result of so-called "phishing" emails sent by fraudsters impersonating credible institutions to steal personal or financial information via a contaminated link.

Card-Present-frauds: This is less common today, but it's still worth watching out for. It often takes the form of "skimming" – when a dishonest seller swipes a consumer's credit card into a device that stores the information. Once that data is used to make a purchase, the consumer's account is charged (graphic.com.gh, 2017).

- **Social Engineering**

Social engineering is a method in which cybercriminals make a direct contact with people through phone calls, emails, or even in person. Basically, they will also act like a genuine people. They will befriend you to earn your trust until you will provide your important information and personal data. They will in tend use this personal biodata to defraud people and bigger companies after winning their trust (Hatfield, 2019). Hatfield (2019) further articulated that the reason why cybercriminals usually uses social engineering formats is that they think is much easier to win people trust more quickly than to learn means of cracking their software or accounts details. To lure people to getting their password through face to face or verbal contact is simple and easier than trying to hack their passwords and other personal details.

2.10 Cybercrime Legislations in Ghana

Technological advancement coupled with free digital information has resulted in a steady increase of online crime in varied formats. These crimes could be very difficult to address without involving legal structures and law enforcement agencies of the state. Brenner (2010) disclosed that online crimes have posed a number of questions in the minds of the general public, the government and the security apparatus in the country. Brenner (2010) further noted that because electronic transactions are transboundary in nature it is often difficult to determine which cybercrime activities are legal and which are not. What is legal in one country may not be legal in another country. For instance, hacking alone does not constitute a crime in Brazils laws, any fraudulent act must be proven for prosecution (BBC, 2004) as cited in (Boateng *et al.*, 2010). It seems almost impossible to proofing a virtual crime. Virtual or online business poses the question of relativity in terms of location and the laws. Because of the seizer of the cyberspace by cybercriminals, nations have developed laws, acts and bills through their legislative instruments to deal specifically with the menace of cybercrimes.

Most nations depended on their existing laws in dealing with cybercrimes and other computer related crimes. For example, in 1988, for instance, the United Kingdom House of Lords ruled that unauthorized access to a computer system did not constitute an offence under existing criminal law (Goodman & Brenner, 2002). Meaning that, their past laws did not consider illegal and unofficial usage of computers of others as a crime until now. Again, in the United States Senate Governmental Affairs Committee also passed the Federal Computer Systems Protection Bill in 1976. It was reviewed and reinstated in 1979. Article 139 of the reviewed bill affirmed that “knowing, willful, manipulation or attempted manipulation of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce, for the purpose of devising or executing any scheme or artifice to defraud, or of obtaining money, property, or services by means of false or fraudulent presences, representations, or promises to be a crime and could have a jail sentence of up to 15 years” (Goodman &

Brenner, 2002). The country came out with 'Computer Fraud and Abuse Act (CFFA)' in 1984 to substitute the Federal Computer Systems Protection Act. Before 2008, Ghana had no law on cybercrime, so cybercriminals were handled like any common criminal by the police. However, Ghana's acknowledgment to the existence and reality of cybercrime posing as big threat to the country's economy the government of Ghana have taken steps to combat it in 2008. Ghana initiated Electronic Transactions Act (2008) (Act 772) to illegalize computer hacking and pave the way to the appropriate agencies to deal decisively with suspected cybercriminals (Abem, 2013). Cybercrime is increasingly posing a real threat to Ghana. The government of Ghana, through the Ministry of Communication has come out with some Acts to regulate the conduct of people in the cyber space. Credence is given by speeches delivered by both present and past Communication Ministers of Ghana. Minister of Communication (Mr. Haruna Iddrisu) in a speech in 2009 remarked that alternative Cyber Crime Response Team has been put in place, to take a second look at the current laws of the information communication and technology (ICT) databases to strengthen the country cyber space system. He appealed the criminal investigation department (CID) to fortify the capability of the e-Crime Department of the Ghana security agency in an effort to curtail cybercrime in Ghana (GNA, 2009). Addressing the media at Meet the Press series in Accra (2018) by the Communication Minister (Ussal Owusu-Ekuful) reported that a survey carried out by the World Bank and the Global Cyber Security Capacity Centre of the Oxford University on Ghana's cyber security maturity level have shown that "we have a long way to go." Attempt to move the country to virtual and paperless society by establishing e-services have made Ghana a potential cybercrime target. Actions such as the formation of the National Cyber Security Centre to coordinate cyber security activities in the country have been introduced. Ussal Owusu-Ekuful further stated that considering the rising case of cybercrimes aiming at the banking industry, Bank of Ghana is teaming with the Ministry of Communications and the Association of Bankers launched a "Cyber and Information Security Directive for the Financial Industry to support cyber risk management in the financial sector". Again, she said Ghana has signed to two significant international agreements on cyber security "The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and The Convention on Cybercrime (Budapest Convention)". These two international treaties are aimed to heighten Ghana's collaboration with other nations towards policy, technical and operational levels in tackling cybercrime and other cyber security deficiencies (graphic.com.gh, 2018).

Ghana National Cyber Security Policy & Strategy (GNCSPS) reported that some websites such as "Ghana's official web portal, National Communication Authority, National Information Technology Agency and the website of the vice president of Ghana" have all been mutilated in Ghana from existing as a results from cyber-attacks. These have dented the good reputation of Ghana and call for swift action to mitigate some of these attacks from recurring in future (GNCSPS, 2014). These have necessitated the country to activate its legislative arm to pass some laws, acts, programmes to deal with these threats of cybercrime and its forms. These include; The Electronic Transaction Act (ETA) 2008, the Data Protection Act, National Cyber Security Awareness Programme, National Cyber Security Centre, National Cyber Security Council, National Cyber Security Working Group, National Cyber Security Crisis Management Plan, Computer Emergency Response Team, Computer Security Incidence Response Team, Electronic Communications Act, National Communications Authority and National

Information Technology Agency. GNCSPS (2014) concluded that, all these acts, laws, bodies, programmes, organisations and treaties are authorised in various ways to handle cybercrime to smoke out cybercriminals in all sectors of the Ghanaian economy.

2.11 Causes of Cybercrime

Cybercrime is one of the most common and prevalent among the youth which affects many countries in the world. This is caused by many factor and the culprits are warmly welcome and received by certain individuals and social institutions after making money through this unapproved means (Ninalowo, 2016). People attribute causes of cybercrime to many reasons which includes;

- **Attitude of Getting-Rich-Quick**

Every human being have choice to make in live which could either be good or bad choice. However, some people choose to cut through the illegal ways of making money. Shehu (2014) revealed that most people especially the poor want to bridge the wider gap of poverty through cybercrime. They are very keen in making money by all means possible within the shortest period of time which often pushed them to cybercrime. Meke (2012) indicated that people who are poor are more engaged into cybercrime than the rich people. Poverty is evil and has a direct relationship with crime. Poor people are more vulnerable to committing crime than the rich people.

- **Growth in E-commerce and E-businesses**

Serianu, United State International University-Africa (2016) in Ghana cybersecurity report testified that, there is a high growth in electronic business. Most financial institutions have move to electronic banking system and cashless transactions. These initiatives comes with some level of risk which gave birth to online scams, ATM skimming and identity theft.

- **Weak Cybercrime Laws/ Legislation**

Okeshola and Adeta (2013) believed that, menace of cybercrime prevail more on places where there are not strict and stringent laws to deal precisely with cybercriminals. Perpetrators of cybercrime mostly go unpunished which could motive other people to practice cybercrime. Ani (2011) concluded that weak laws inspire people to ignore the consequential effects of committing virtual crime.

- **Unemployment**

There is so much risk and evil associated with youth not engage in any productive economic activity. High rate of youth unemployment can easily influence the youth to engage in crimes such as stealing, robbery, and cybercrime (Okeshola & Adeta, 2013; Warner, 2011).

- **Parental Control**

Lack of parental control is another cause of cybercrime. Evidence from Adejoh, Alabi, Adisa, & Emezie (2019) disclosed that some parents indirectly support their children by ignoring interrogate means of sustenance. Some parents refuse to report crimes of their children to the police when they are aware that their children are into cybercrime. Some have no idea on what kind of work their children engage to make money whether legal or illegal means.

- **Accessibility to Internet and Technology**

Easy access to internet bandwidth coupled with availability of personal computers and other hand held mobile gadget offer people the opportunity to commit various types of online crimes (Aiken, Davidson & Amann, 2016; Adejoh *et al.*, 2019).

- **Vengeance or Payback**

Most young cybercriminals or sakawa boys try to justify their thievery actions. Warner (2011) revealed that, in Ghana most of the sakawa youth believe that they paying back to the white men for taking our gold and our great grandparents. This is the only means we can get them pay for what they did to us. This is the redistribution of wealth and social justice. The only we can avenge for our forefathers is through this means (Okeshola & Adeta, 2013).

- **Peer Pressure**

Peer group is very effective and influential. Confirmation form Adejoh *et al.* (2019) and Obiri Yeboah (2015) revealed that, youth that are involved in this scamming business are students. They are group of desperate youth who have seen their colleagues made through cybercrime so they try to emulate them. They see their peers living in flamboyant lifestyle, driving nice cars, putting on nice dresses and watches so they too want to look exactly like their friends and they finally join in whatever their friend are in to.

- **Fame/ Societal Recognition**

Fame is another incentive package which drives young people into cybercrime. Hassan *et al.* (2012) identified fame as one of the causes of cybercrime. Some societies put much recognition and weight on people with money and properties. Such societies celebrate wealth without questioning their source and held such people in high esteem. This act drives people into cybercrime.

2.12 Effects of Cybercrime

For the past years cybercrime have cost a lot of destruction to many countries, organization and individuals across the globe. Button, Lewis & Tapley (2014) articulated that, cybercrime is a worldwide threat and every patron of cyber-enabled tools as well as e-businesses is prone to the victimisation of cybercriminals. The effects of this cybercrime menace are huge and devastating. Unlike other crimes, this form of crime is limitless in scope which possesses a multiple effects on the victim and society at large. Some of the effects are discussed below:

- **Emotional or Psychological Effects**

The effects are usually emotional or mentally and vague in nature. Evidence from Brody and Perri (2016) indicated that, most victims neglect to report their cases because of depression and shame, stupid or greedy to narrate their ordeal to authorities who can take legal actions. This makes it often difficult to take legal action against victims. Most victims are frustrated and resort to drugs and other unacceptable lifestyle and in worse cases victims commits suicide.

- **Data and Financial Lost**

Companies and individuals are losing money and valuable information through cybercrime. According Morgan & Park (2019) the effects of cybercrime is so endemic which ranges from data damages, stealing of funds and assets, intellectual property theft, identity theft, financial theft and many others. They established that cybercrime epidemic will lead to global loss of six trillion dollars yearly by 2021, double increase from three trillion dollars in 2015.

- **Defamation of Image**

Cybercrime gives bad image to countries that are mostly engaged it. Okeshola & Adeta (2013) stated that Nigeria has been listed as one of the countries in the world with high cybercrime dominance in the world. This has stained the good reputation of the country. Most foreign investors are afraid to invest and do business in places with this negative tendency

- **Loss of Life**

Most of the youth engaged is cybercrime in Ghana often resort spiritual means to ensure continues flow of their financial success. Warner (2011) proof that, many deaths and injuries over the past years have been blamed on sakawa boys in Ghana. There have been cases of some of them been paralysed in the process of performing sakawa rituals, murder, kidnappings, and removal of genitals by these cybercriminals for rituals.

- **School Dropout**

Many students are dropping out of school to concentrate on making money through cybercrime. Oluwadare, Oluwasanmi & Igbekoyi (2018) stated that Nigeria educational system is in deplorable state by proliferation of cybercrime culprits into the system. Currently, most students in Nigeria prefer materials they obtain from cybercrime to schooling making them dropouts and lazy to develop the culture of reading.

2.13 Cybercrime and Educational Progress

Crime seems to be a perpetual act in our contemporary civilisation. Even though laws and socials workers trying and working hard to reduce it. The Northern Regional Director of Education in Ghana, Alhaji Mohammed Haroon Cambodia explained that "after registering for the Basic Education Certification Examination most of the final year students no longer report to school but rather engage in vices that only land them in trouble. He said the students mainly engage in hooliganism, watching of pornographic films, internet fraud popularly known as “sakawa”, sexual immorality and all manner of indiscipline” (Ghana news agency, 2017). Daniel (2015) opined that in Ghana, the term “sakawa” has been used to describe cybercrime which is considered as a big crime in the country. Children between the ages of 10 – 15 mostly at school going age are seriously involved in this illegitimate act. Reports in our dailies give credibility to the fact that cybercrime threatens the educational progress of children under school going age in Ghana. School schoolchildren often leave the classroom for internet cafés in order to be involved in the act. This affects academic progress as those involved fail to attend school for a considerable period of time. The perpetrators engage their partners (victims) in a persuasive dialogue over a period of time, falsify documents, and create a situation that convince victims to either transfer money or make available their credit card details to them (Ghana news agency, 2017).

Igba, Igba & Nwambam (2018) articulated that technology offers humanity with the greatest important benefit which leads us a considerable amount of danger and risk. By a click of a button one can access and share quite substantial amount of information to people and organisations across the globe. Undoubtedly, this can be so damaging when it is misapplied. In the case of internet the danger of on risking privacy, identity, property and many more is so high. Some of these cybercrimes include cyber terrorism, theft and fraudulent use of personal information counterfeiting, credit card crimes, pornography and hacking to mention but a few, all these have effects on senior high school students. Almost 77% and 68% of urban and rural families respectively in Nigeria are measured poor. According to Federal Republic of Nigeria (FRN, 2013), national strategy on education, the larger majority of students are from the poor rural family background in Nigeria. This has negative influence on the academic progression of such students and it enticed them to cybercrime where they can easily make money. The availability of computers and internet has a direct impact on education and national development (FRN, 2013). Oluwadare, Oluwasanmi & Igbekoyi (2018) stated that Nigeria educational system is in deplorable state by proliferation of cybercrime culprits into the system. Currently, most students in Nigeria prefer materials they obtain from cybercrime to schooling making them lazy to develop the culture of reading. Unexpectedly, in the present-day, the significance of ICT has taken a different toll amongst undergraduate students in some state universities in Nigeria. This has been proven through the use of internet to defraud people known as cybercrime. The internet aid as a hideout for students fraudsters who have exclusively moved from the streets to an electronic platform (Adeleke, 2017). Dashora (2011) articulated that the main reason why most school children engage in cyber criminality is to satisfy their curiosity to know, learn and to discover things through the internet. They also want to demonstrate to their peers that they are outstanding amongst them.

2.14 Legal Approaches to Combat Cybercrime

Legal measures are usually considered as possibly the most relevant aspect of cybercrime control. Such measures include the establishment of laws which prohibit acts that violate the security or integrity or availability of computer data and systems or networks and attacks against critical information infrastructure (Orji, 2018). In most nations of the world, including Sub-Saharan Africa (SSA), there are two main primary stake holders who are fully engaged in the fight against cybercrime. These are; law enforcement agencies which consist of both the national and international police and the anti-crime commissions made of commissions from various national states and regional blocs (Akuta, Ong'oa and Jones, 2011).

There are various national and international organized bodies and organizations which are at the fore front in trying to combating cybercrime namely: the Economic Community of West Africa States (ECOWAS), European Union (EU), Unite Nations (UN), various National Assemblies, Law Enforcement Agencies, the Judiciary Systems, Crime Commissions, and the International Police (INTERPOL) (Akuta, Ong'oa and Jones, 2011).

- **European Union (EU)**

The European Union (EU) with the assistance of Europol has implemented many platforms and legislations to fight cybercrime and other computer related crimes. These platforms are meant to track and gather intelligence on cybercrime committed in various Member States (Orji, 2018). The Commission of the European Communities presented on April 19, 2002 a proposal for a Council Framework Decision on attacks against information systems. The proposal was adopted by the Council in 2005 and includes Article 2: Illegal access to Information Systems, Article 3: Illegal System Interference and Article 4: Illegal Data Interference. The European Union Commission again in May 2007 thought of creating legislation on identity theft to be known and called: "Towards a general policy on the fight against cybercrime." The Commission called for Cybercrime Expert Meeting to discuss steps in implementing a comprehensive policy of framework to fight cybercrime. A statement was made as follows: "The increasing prevalence of cybercrime across Europe, spanning large scale attacks in Estonia, identity theft in Spain, illegal content and high-profile online child abuse incidents in Austria, Germany, Italy and the UK, highlights the need for concerted action. Indeed successful operations such as "Operation Koala" and the global hunt for "Vico" pedophile depends on regional and international cooperation. The conclusions of today´s meeting represent an important step by the EU to establish the cooperative links upon which success is build" (European Cybercrime Law, 2013).

The Council of Ministers of the European Union adopted in November 2008 the Councils strategy to reinforce the fight against cybercrime. The new strategy recommends: “reinforcing partnership between the police and the private sector by better knowledge-sharing on investigation methods and trends in cybercrime. It also encourages both parties to respond quickly to information requests, resort to remote searches, cyber patrols for online tracking of criminals and joint investigations across borders. The strategy also calls for the setting up an alert platform in the short term, where reports on crime committed on the Internet, such as posting of illegal content, in EU would be pooled for cross-checking by Europol.” Europol was requested to implement the platform. The Commission further in 2009 came out with a message on establishing Critical Information Infrastructure Protection (CIIP) entitled “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.” Also, in 2012, a conclusion to establish European Cybercrime Centre (EC3) was submitted. This was endorsed by Council with title “Tackling digital crime through the establishment of a European Cybercrime Centre - The way forward” (European Cybercrime Law, 2013).

- **Council of Europe (CoE)**

Council of Europe Convention (CoEC) (2010) on Cybercrime set a very important landmark in the combat against cybercrime. This convention came into force on July 1, 2004. Many countries had endorsed and ratified to the Convention in order to enable them fight cybercrime effectively. By subscribing or ratifying to the Convention, the States approve to confirm that their domestic laws criminalize the conducts described in the substantive criminal law section. This Convention set as benchmark and reference point for these countries developed their own international legislations to fight cybercrime. The Convention often adopts and updates new methods of conducts in cyberspace with criminal intent to cover modern forms of cybercrime. The council deems it very important to implement at least Articles 2-9 in the substantive criminal law section. These Articles (2-9) are covered by the explanatory report of the Council of Europe Cybercrime Convention. These are; Explanatory comments on illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud and offences related to child pornography are available (CoEC, 2010).

Article 10 deals with specifically on identity theft. This Article deals with criminals who misuse personal information belonging to another to commit fraud. However, the loss or theft of the information itself does not ordinarily constitute a criminal offence. Some countries use the term “identity theft” when perpetrators obtains financial information or personal identification information of another individual. The new Penal Code in Norway (2009) avoids the term “theft”, using a substitution such as “identity infringement” (CoEC, 2010). This form of crime was known before computers came into existence.

With advent of information and communication technology, it has turned into a very dubious lucrative business for criminals. Masses of people across the globe suffer the financial and emotional trauma and pain of identity theft. In most countries, no legislation exists covering identity theft. One exception is the United States, where federal legislation and almost all states have adopted laws on identity theft that may also be applied against criminal conducts through computer systems (Schjolberg & Ghernaouti-Helie, 2011).

- **International Police (INTERPOL)**

The INTERPOL has been very instrumental and cooperative in the fight against cybercrime and other related crimes around the world. In the history of police investigation of computer crime and cybercrime INTERPOL has since the 1980s been the leading international police agency in this field. INTERPOL has established Regional Working Parties for local regions in Africa, Asia, Latin America, and Europe. The working parties comprise of team and heads of experienced members of national computer crime units. INTERPOL also organize international conferences, seminar and workshops on cybercrime for the global law enforcements, and global training courses specializing in cyberspace investigations such as investigations of botnets, malicious codes and cases where Voice over IP is involved (INTERPOL, 2011).

INTERPOL also formed a very formidable rapid information exchange system for cybercrimes, an international 24/7 response system including National Central Reference Points (NCRPs) in over 120 countries for a global cooperation on cybercrime investigation. This system has been endorsed by the G8 High Tech Crime Sub-group. The 24/7 system enables police in one country to immediately identify experts in other countries and obtain assistance in cybercrime investigations and evidence collections. INTERPOL Global Complex Innovation (IGCI) based in Singapore has a 24-hour Command and Co-ordination Centre (CCC) which was established and commissioned in 2014 to help in global surveillance on cybercriminals (IGCI, 2014).

- **G8 Group of States**

The Group of Eight (G8) originate in 1975 is regarded as highly industrialized states in the world which includes France, Germany, Italy, the United Kingdom, Japan, the United States, Canada, and Russia. The G8 established Subgroups of the Lyon Group. One group in the subgroups was the G8 group of High-Tech (U. S. Department of Justice, 2004). At the meeting in Washington in 1997 G8 propose Principles to be adopted in the combat against computer crime. They also have 24/7 network for the assistance in global cybercrime investigations. This network comprises of over 40 countries across the globe, and also works in collaboration with INTERPOLs 24/7 network. The aim was to make sure that no criminal hides or receives safe havens anywhere in the world (U. S. Department of Justice, 2004). The G8 have issued and adopt several statements during their meetings to combat against cybercrime and fraudulent use of Internet. At their meeting in a 2004 one of the G8 adopted objectives was: to ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents.

At meeting in 2006: We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work. At meeting in 2009: Criminal misuse of social networks, encryption services, VoIP services, the Domain Name System, and other new and evolving criminal attacks on information systems, pose increased challenges to law enforcement and are spreading (Schjolberg & Ghernaouti-Helie, 2011).

- **African Union (AU)**

Following a massive improvement and growth of telecommunication and availability of wireless and internet bandwidth in Africa has resulted in an increase internet user population. This development comes with miss use and abuse of these facilities. Individuals, businesses and organisations are threatens through the use of internet by criminals and fraudsters in the cyberspace (Miniwatts Marketing Group, 2017).

This has raised serious concerns over the need to promote cybersecurity governance and cyber stability in the continent. This has call for the adoption of Convention on Cyber Security and Personal Data Protection, in June, 2014 by African Union (AU). The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime (Orji, 2018). The Declaration further directed the AU to "jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a Convention on cyber legislation based on the continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cybersecurity, and personal data protection." Under the Convention, the obligations to establish national cybersecurity governance structures requires the establishment of appropriate national institutions with responsibilities to tackle cybercrimes and respond to cybersecurity incidents, and also facilitate international cooperation in the management of such incidents. Thus, within the context of those obligations, it is implied that every Member State should establish institutions such as a national cybersecurity agency and a national Computer Emergency Response Team (CERT) (UNECA, N. D.).

2.15 Conclusion

This chapter reviewed literature from various credible related sources from global to local levels. It also discussed the various theoretical frameworks which underpinned the study, forms of cybercrime, cybercrime legislations in Ghana, causes and effects of cybercrime and cybercrime and educational progress.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter takes into consideration research methods that are used in the study and how the study was carried out. It also describes the research design, population, sampling methods, instruments for data collection and methods of analysing data.

3.2 Study Area

Vitting Senior High Technical School is a non-faith community based co-educational day/ boarding school located off the Tamale-Yendi Road about 400 m from the Tamale Teaching Hospital. It started as a Middle Mixed School and metamorphosed into a Junior Secondary School until it assumed its present status of Vitting Senior High/ Technical School. To become the hub of innovative, practical technical and vocational education of the 21st century, the school equips the individual students with nouvelle employable and entrepreneurial skills to compete with ease in the ever changing market. Mission to maintain and motivate qualified reflective thinking staff to instill discipline, nurture entrepreneurial and leadership skills, and deliver lessons in a student friendly atmosphere with the state of the modern art in various study programmes.

3.3 Research Design

A research design is a plan that concern about best strategies, techniques and resources for research or a study (Hakim, 2000). This helps in the data collection in order to answer research questions. It provides the structure or framework for data collection. The most common research designs are experiments, surveys or case studies. This study adopted case study design. A case study design is a "scientific method of study which involves observing, describing, collecting and recording of the behaviour of respondents without influencing them in any way" (Creswell, 2013). This approach was adopted to attain the overall views of participants. Creswell (2014) stated that case study pays much attention to details which examined and analysed the questions and proposals raised about the issues or phenomenon under study. It also assists to map out specific borders of the case and gives much precision of issues form the start to finish of the case study.

The reasons for employing a case study design is that the study attempts to explore a progressive and recurrent social phenomenon in a real life situation to collect empirical data and to communicate them as they are obtained. Case study design is regarded as more fitting and suitable. Additionally, Boateng (2014) concluded that a case study permits for "empirical investigations of a particular contemporary phenomenon within a real life context, using multiple sources of evidence" such as questionnaires, interviews and documentary analysis.

3.4 Research Approach

The mixed methods approach was adopted by researcher. This method combines both qualitative and quantitative technique in collecting and analysing the data for the study. Boateng (2014) stressed that researchers have the ability to select from the three main research approaches which includes qualitative, quantitative and mixed method. Creswell (2013) explained that mixed methods complement each other and offer deep understanding of data collected especially in qualitative data and also broaden the understanding of research problems. Considering the sensitivity and social nature of the phenomenon under study the mixed method was much appropriate to use. The study comprises many people and also criminality in nature so connecting quantitative and qualitative approaches were superior option. Each approach exhibits distinctive features in handling multiple circumstances and issues of this nature of phenomenon.

3.5 Study Population

The target population was form one to form three students in the Vitting Senior High School. Vitting Senior High School was selected due to its close proximity and because of the speculation that "Vitting is a popular haven for scammers/ shatters". The Senior High School (SHS) students are considered because this is a very critical stage in progressing in the academic ladder in the Ghanaian educational system. Vitting Senior High School has a total of 1,947 students that are spread out in two different tracks (green and gold) and levels from form one to three. The study therefore concentrated on the gold tracks (form one and two) which were in session and the whole of form three which is not part of the double track system.

3.6 Sample Size

Sample size of 329 respondents was obtained using the Yamane formula (that is N $=\frac{\mathrm{N}}{1+N(e^{2)}}$). In this regard, a 5% margin of error was assumed, with estimations set to be within 95% confidence interval. The formula is shown as:

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

$$\mathrm{N} = \frac{50}{1+50(0.05^{2)}}$$

$$\mathrm{N} = \frac{50}{1+50(0.0025)}$$

$$\mathrm{N} = \frac{50}{1.125}$$

N = 44

N = population size of the study group. One (1) = is a constant number, e = margin of error (is the desired level of precision which is assume as 5% expressed as 0.05). The above calculations were done for each class which was chosen at random to get the total sample size of three hundred and thirteen (313). To take care of contingencies and non-responses, a 5% margin was allowed on the calculated sample (5/100 multiply by 313 = 16). This brought the actual sample size to 329.

Table 3. 1: Selected Programmes for the Research

Class/Form	Programme	Total	Computed Sample Size
SHS 1	Agriculture	50	44
SHS 1	Technical	58	51
SHS 2	Visual Art	53	47
SHS 2	General Art	79	67
SHS 3	Home Economics	52	46
SHS 3	Technical	68	58
Total		**360**	**313**

3.7 Sampling Procedures

A stratified sampling procedure was employed in the study. This technique was used to draw conclusion from different levels or strata. Stratified sampling technique was adopted where levels (form 1, 2 and 3) were represented as strata/ stratum. The class register for the three levels (SHS1, SHS2 and SHS3) were obtained from the head teacher in charge of academics. Portioning and distribution of respondents from various levels or strata was proportionately determined.

In the final stage, simple random sampling technique was used in selecting the respondents from each strata. This was done to ensure that the findings of the study will be representative of the population which could be used for generalisation. Purposive sampling was also used to select the Assistant Headmaster in charge of academic and the Senior Housemaster of the school for key informant interview. This is because they are directly connected to the students. The headmaster in charge of academic possesses some level of knowledge about the entire student body regarding their academic records. The senior housemaster on the other hand monitors the entire students body in order check and truck any truant behaviours among them. Sarantakos (2013) declared that purposive sampling technique offers the researcher an opportunity to choose subjects who possess some special knowledge relevant to the study.

3. 8 Sources of Data

The researcher collected information from both primary and secondary data. Data from the primary source was produced from the answers of the participants. The secondary source of information came from Tamale Metropolitan Assembly, books journal articles, published theses and the internet sources which were significant to the study.

3.9 Instruments and Data Collection

There are various devices that researchers can use to collect information which are called instruments. In this study, data was collected using questionnaire and an interview guide. Key (1997) explained that questionnaire is most frequently a very brief, preplanned set of questions prepared to solicit specific information to meet a particular need for research information about a pertinent topic. An interview is a direct face-to-face attempt to obtain reliable and valid measures in the form of verbal responses from one or more respondents

(Key, 1997). The questionnaire was used as a means of collecting quantitative data. Walliman (2015) stated that quantitative data exhibits "features that can be measured, more or less exactly". Burns and Grove (1993) define quantitative methodology as official, impartial and orderly procedure to define and test relations and connections between two or more variables or groups. Using questionnaire has the following advantages, they are economical, uniformity of questions and easy to collect and analyse in a relatively short period of time (Key, 1997).

Two types of questions were asked, closed-ended and open-ended. The close-ended gave the respondents options to select responses from given fixed choices. Also, in the case of open-ended respondents have the option to give their own unrestricted opinion, perception and attitudes about questions. The questionnaire was divided in to section to reflect the themes of the objectives. The first section (A) represents the socio-demographic characteristics of respondents and their families. The second section (B) asked questions about the prevalence of cybercrime or sakawa among students. The section three (C) contained knowledge about cybercrime or sakawa of respondents. The next section (D) talks about factors that influence/pull SHS students into cybercrime or sakawa whilst the last part (E) talks about effects of cybercrime or sakawa on the academic performance of SHS school students. They were presented in a modified five-point rating scale thus: Strongly Agree (SA) = 5 points, Agree (A) = 4 points, Neutral (N) = 3 point, Disagree (D) = 2 points and Strongly Disagree (SD) = 1 point.

The interview method was used to gather qualitative data. The interview is a qualitative data gathering instrument which plays an important part of research. It offers the opportunity to gather data which otherwise may not be obtained with other instruments like the questionnaire. The questions were guided by information from the reviewed literature in order to help adequately examine the research questions. According to Pickard (2007) qualitative approach is commonly used in behavioural sciences which are focused on non-numeric (qualitative) data. Qualitative data is not based on nominal and ordinal levels of quantifications. Comparatively, qualitative approach in research is ineffective in terms of identifying, measuring or quantifying and other scientific measurement. This research approach is essential and significant because it allows for opportunity to examine varied human phenomenon in various viewpoints (De Vaus, 2002). Qualitative approach is more suitable for studies involving people and their societies and other attributions. It allows free flow of questions and answers which contributes significant ideas and knowledge to the study. Data cannot be measured or calculated. This is seen as shortcoming in contrast with quantitative method. The researcher personally gathered the information through face to face interview. The questionnaire was administered by the researcher and two teachers from the school were hired.

3.11 Ethnical Consideration

The researcher sent copies of introductory letters from Faculty of Education to the headmaster of Vitting SHS. To comply with research ethics the research brief the respondents on the nature and purpose of the study. Participants were made to understand that participation is voluntary and their anonymity and confidentiality of all information offered are assured. This boosts them to open up to be truthful and to volunteer any information they have about the study. They were also given the chance to asked questions for further clarification.

Honesty, decency and integrity are very essential in conducting research. These factors must be taken into account in order to protect the rights, identity and confidentiality of respondents. To ensure that the study follows ethical details, free will, anonymity, confidentiality, privacy and consent were duly followed. Informed consent is very significant in research. No falsification and manipulation of data in the course of analyzing the results. This is to ensure research and academic dishonesty. The open-ended questions were also cross checked by the supervisor to ensure trustworthiness and reliability.

3.12 Reliability and Validity

Elmes, Kantowitz and Roediger (2011) define reliability as the state of uniformity with which a tool measures a feature it is designated to measure. The answered questionnaires showed some uniformity and consistency in responses. Reliability could also be guaranteed by making sure that errors are avoided, for example biasness of the data collector. This was checked by the researcher educating the other two assistants on the need to be impartial against the respondents which is against the research ethics. They were questioned to portray unique personal characteristics and attribute towards all the respondents, for example openness, friendliness, sociable, care and support. The data was collected in a very conducive manner to offer respondents comfort and privacy. Respondents were demanded not write their names on the questionnaires to conceal their identity for confidentiality purposes.

The validity of a tool or an instrument is the extent to which such tool or instrument is able measures the variables it envisioned to measure (Elmes, Kantowitz and Roediger, 2011). Content validity is the degree to which an instrument covers the concepts and factors of interest under study. This was achieved by including in the questionnaire diversity of questions such as the types, reasons and impact of cybercrime on SHS students. This could also be achieved through uniformity and consistency in the questionnaire's administration. The questionnaire was personally circulated to the respondents which were all written is simply language to the understanding of the respondents. To further validate the questionnaire was given to an expert to read through and make necessary corrections and inputs. At the point of collecting the administered questionnaire from the respondents the researcher and other assistants crossed checked them critically to ensure that the questionnaires are properly answered by the respondents.

3.13 Pretesting and Training

Pretesting refers to a trial version of the real action. This is a trial administration of the questionnaire for identification and correction of errors detected before the final day of its administration to the selected respondents (Elmes, Kantowitz & Roediger, 2011). When an instrument (questionnaire) is used in collecting data it is important to know as to whether the respondents understand the questions and instructions regarding what they are expected to do in answering the questions. Pretesting was done to eliminate all the necessary irregularities and errors which were detected in order ensure the reliability and the validity of the instrument.

Ten of the questionnaires were administered to ten students in Vitting Senior High School by accidental sampling technique and three teachers were also given training for a day to understand the objective of the research, sampling procedure, structure of the questionnaire, checking the completeness of questionnaire.

3.14 Data Analysis

The completed questionnaires were organised, arranged and cleaned by the researcher. Data which was collected from questionnaire were analysed using the Statistical Package for Social Sciences (SPSS). It employed descriptive analysis where summaries were expressed in frequency tabular form and data was presented in pie diagrams and bar graphs for adequate interpretation. The interviews were audio-recorded and transcribed. Qualitative content analysis was used to analyze the data that was gathered from the interview transcripts, and open-ended survey responses. Qualitative and quantitative findings were analysed simultaneously in order to enhance the interpretation of the study results.

3.15 Conclusion

This chapter discussed the methods adopted in the study; research design, research approach, study population, sampling technique, calculation of sample size, instrument for data collection, ethical considerations and data analysis among others were clearly discussed. Survey method was used. Data was collected by means of interviews and questionnaires administered by the researcher from 329 respondents. Permission was sought from the school authorities. Consent was obtained from the respondents. Anonymity and confidentiality were ensured during administration of the questionnaires and report writing.

CHAPTER FOUR

RESULTS

4.1. Introduction

This chapter presents findings of the study in the form of results obtained from the analysis in connection to the study‘s objectives. The study employed triangulation method in the analysis and interpretation of data which was obtained from the field. The study was conducted in accordance with the research objectives with three hundred and twenty-nine (329) students from Vitting Senior High and two (2) key informants were interviewed. The student population who responded to the questionnaire comprised of 253 males and 76 females from first year to final year. All the questionnaires were retrieved for the analysis and presentation of results. The findings were presented using tables, charts with major headings under the various specific objectives. The main statistical methodologies used in the analysis, interpretations and presentations were: frequency distribution tables, multiple response analysis and correlation.

4.2. Socio-Demographic Characteristics of Respondents

This section presents the socio- demographic attributes of the respondents. The attributes are gender, age, custody of respondents, marital status of respondents' parents or guardians, educational level of respondents' parents and many more. Majority of respondents 253 representing 76.9% were males whereas 76 representing 23.1% were females (Table 4.1). The age distribution of respondents ranged between 13 - 15 years were 39.5% (130), 16-18 years were 39.8% (131), 14.9% (49) were between 19-21 years and 22 - 24 year were 5.8% (19) (Table 4.1).

Table 4. 1: Demographic characteristics of respondents

Demographic characteristics	Frequency	Percentage (%)
Gender		
Male	253	76.9%
Female	76	23.1%
Total	329	100%
Age		
13 – 15	130	39.5%
16 – 18	131	39.8%
19 – 21	49	14.9%
22 – 24	19	5.8%
Total	329	100%
Custody of respondent		
Father	42	12.8%
Mother	95	28.9%
Both parents	135	41%
Guardian	57	17.3%
Total	329	100%
Marital status of respondent parents or guardian		
Single	26	7.9%
Married	165	50.2%
Divorced	63	19.1%
Separated	74	22.5%
Total	329	100%
Educational level of respondents parents or guardians		
None	146	44.4%
Primary	83	25.2%
JHS	70	21.3%
SHS	16	4.9%
Tertiary	14	4.3%
Total	329	100%
Course of respondents		
Agriculture	44	13.4%
Home economics	46	14%
Technical	125	38%
Visual art	47	14.3%
General arts	67	20.4%
Total	329	100%
Level or form of respondents		
SHS 1	95	28.9%
SHS 2	130	39.5%
SHS 3	104	31.6%
Total	329	100%
Residential status of respondents		
Day	66	20.1%
Boarding	262	79.6%
Hostel	-	-
Total	329	100%

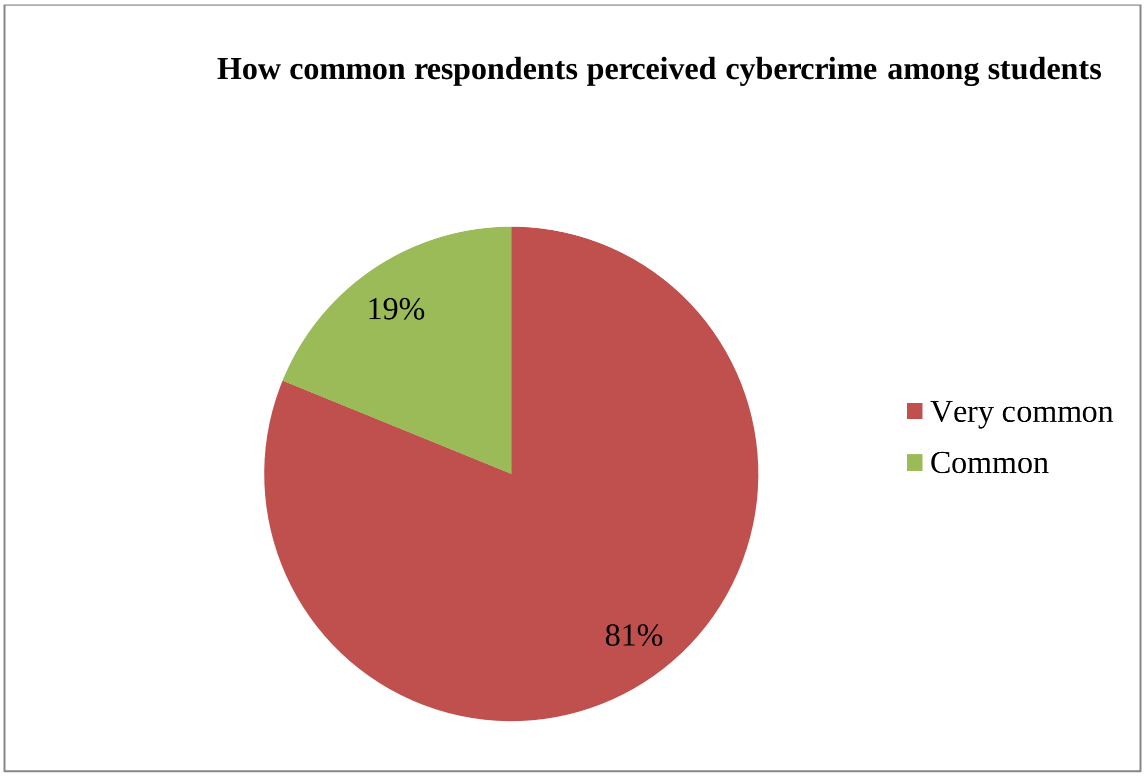
Source: field survey, 2020

The survey revealed 135 of respondents representing 41% are living with both parents, 95 respondents representing 28.9% live with their mothers, 57 respondents which is 17.3% live with guardians whilst 42 representing 12.8% being the least live with their fathers (Table 4.1). The study shows 50.2% (165) of the respondents' parents are married followed by 74 respondents which represents 22.5% were separated, 63 respondents 19.1% are divorced whilst 26 representing 7.9% were still single (Table 4.1). The results shows respondents' parents of 146 representing 44.4% never had any formal education whereas 83 representing 25.2% had primary education, 70 respondents representing 21.3% have had JHS education whilst 16 and 14 representing 4.9% and 4.3% had SHS and tertiary education, respectively (Table 4.1). Also, the level/ form of respondents with percentage of respondents 130 representing 39.5% were in year two, 31.6% (104) in year three whilst the least year group was form one 95 with a percentage of 28.9% (Table 4.1). The survey revealed 262 of respondents representing 79.6% of the total respondents are residing in the boarding house whereas 66 representing 20.1% are day students (Table 4.1).

4.3. Perceived Prevalence of Cybercrime among Respondents

To ascertain the perceived prevalence of cybercrime among students of Vitting SHS respondents were asked to choose from a set of options on how they perceived the level of prevalent of cybercrime among students. In this regard the list of options were very common, common, not common and non-existence for respondent to specify the frequentness of cybercrime or otherwise. From Figure 4.1 below, it is indicated that a greater number of respondents totaling 267 representing 81.2% of the respondents specified that cybercrime is very common among students whilst 62 of the respondents being 18.8% indicated that cybercrime is common. There was no response for not common and non-existence.

Figure 4. 1: Showing How Common Respondents Perceived Cybercrime among Students



Source: Field survey, 2020

4.4 Perceived Knowledge Level of Respondents on Cybercrime

Table 4.2 below covers the result of the responses on the perceived prevalence practices at which students engaged in cybercrime. The table showed that respondents strongly agreed that students who are engaged in cybercrime do the following: Students sent e-mails to impersonate credible institutions to steal personal or financial information via a contaminated link; majority 159 of respondents representing a percentage of 48.3% strongly agreed that some students use the credit card of other people illegally to buy goods and services online, 155 respondents which is 47.1% agreed and 2 respondents representing 0.6% strongly disagreed. Students deceive and manipulate investors resulting in stealing of capital through fake documentation, more than half of the respondents 222 representing 67.5% agreed to this practice, 34 representing 10.3% strongly agreed, meanwhile 65 respondents representing 19.8% were neutral and 8 respondents representing 2.4% strongly disagreed (Table 4.2).

Students steal trade secret, suppliers' agreement, personal records, research documents, to order for goods and services online; 143 respondents representing 43.5% strongly agreed, majority of respondents 147 representing 44.7% agreed, 36 respondents representing 10.9% were neutral, whereas 2 and 1 respondents representing 0.6 and 0.3% strongly disagree and disagreed, respectively (Table 4.2). Students do send email to internet users portraying themselves as legitimate business owners to scam users into giving out private information that will be used for identity theft; more than half the respondents 192 representing 58.4% agreed, 95 respondents representing 28.9% strongly agreed, 34 respondents representing 10.3% were neutral whereas 8 respondents representing 2.4% strongly disagree. Students use special hacking software to infiltrate financial institutions records on the internet; more than half (198, 60.2%) of the responded agreed and 113 respondents representing 34.3% were neutral (Table 4.2). Students buy goods and services online without paying; majority of respondents (169, 51.4%) agreed and 96 respondents representing 29.2% strongly agreed whereas 64 respondents representing 19.5% said neutral (Table 4.2). Students use international money transfer agencies (that is western union and money gram) to carry out a scheme to defraud people; 144 respondents which represents 43.8% agreed while 118 respondents representing 35.9%

strongly agreed whereas 61 respondents which represents 18.5% were neutral and 6 respondents representing 1.8% disagree (Table 4.2). Students persuade people to invest in a non-existent business on the internet, example gold; greater proportion of respondents 138 representing 41.9% agreed. Meanwhile, 119 respondents which represent 36.2% strongly agreed and 48 respondents representing 14.6% were neutral whereas 24 respondents representing 7.3% disagreed (Table 4.2). Students use dating sites to deceive and manipulate people resulting in stealing of capital; majority 128 respondents representing 38.9% strongly agreed while 124 respondents representing 37.7% agreed, whereas 73 respondents representing 22.2% strongly disagree whilst 4 respondents showing 1.2% disagreed (Table 4.2).

Table 4. 2: Perceived prevalence practices of cybercrime/sakawa among respondents.

Practice	Total	Strongly agree	Agree	Neutral	Disagree	strongly disagree	Total
Students sent e-mails to impersonate credible institutions to steal personal or financial information via a contaminated link.	**329**	48.3%	48.3%	3.3%	0%	0%	**100**
Students use the credit card of other people illegally to buy goods and services online.	**326**	38.0%	47.1%	14.3%	0%	0.6%	**100**
Students deceive and manipulate investors	**329**	10.3%	67.5%	19.8%	0%	2.4%	**100**

resulting in stealing of capital through fake documentation							
Students steal trade secret, suppliers' agreement, personal records, research documents, to order for goods and services online.	**329**	43.5%	44.7%	10.9%	0.3%	0.6%	**100**
Students do send email to internet users portraying themselves as legitimate business owners to scam users into giving out private information that will be used for identity theft	**328**	28.9%	58.4%	10.3%	0%	2.4%	**100**
Students use special hacking software to infiltrate financial institutions records on the internet.	**329**	5.5%	60.2%	34.3%	0%	0%	**100**
Students buy goods and services online without paying	**329**	29.2%	51.4%	19.5%	0%	0%	**100**
Students use international money transfer agencies (i.e. western union, money gram) to carry out a scheme to defraud people.	**329**	35.9%	43.8%	18.5%	1.8%	0%	**100**
Students persuade people	**329**	36.2%	41.9%	14.6%	7.3%	0%	**100**

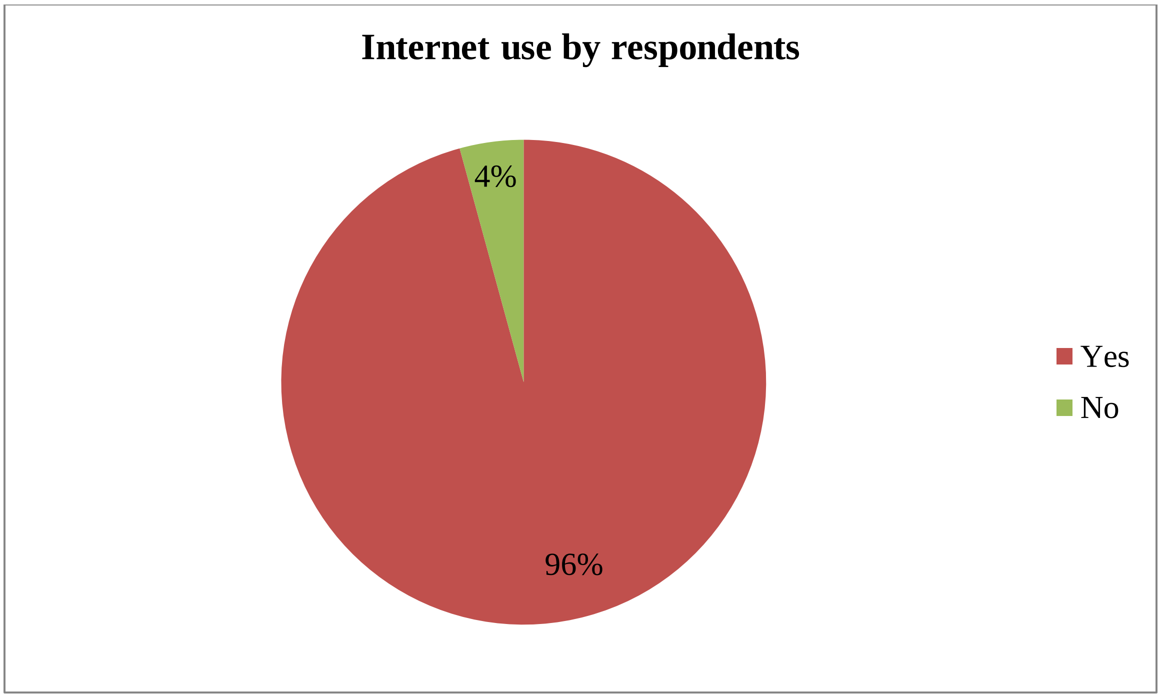
to invest in a non-existent business on the internet, e.g. gold							
Students use dating sites to deceive and manipulate people resulting in stealing of capital.	**329**	38.9%	37.7%	0%	1.2%	22.2%	**100**

Source: Field survey, 2020

4.4.1 Use of Internet by Respondents

To establish the perceived level of knowledge of respondents on cybercrime, respondents were asked to confirm whether they browse the Internet. This is illustrated on Figure 4.2 below. Almost all the respondents 315 representing 95.7% said yes whereas 14 respondents representing 4.3% said no. Interestingly, respondents were further asked to confirm whether they have e-mail or Facebook accounts. More than half of respondents 279 which represents 84.8% said yes whilst 50 respondents indicating 15.2% said no.

Figure 4. 2: Use of Internet by respondents

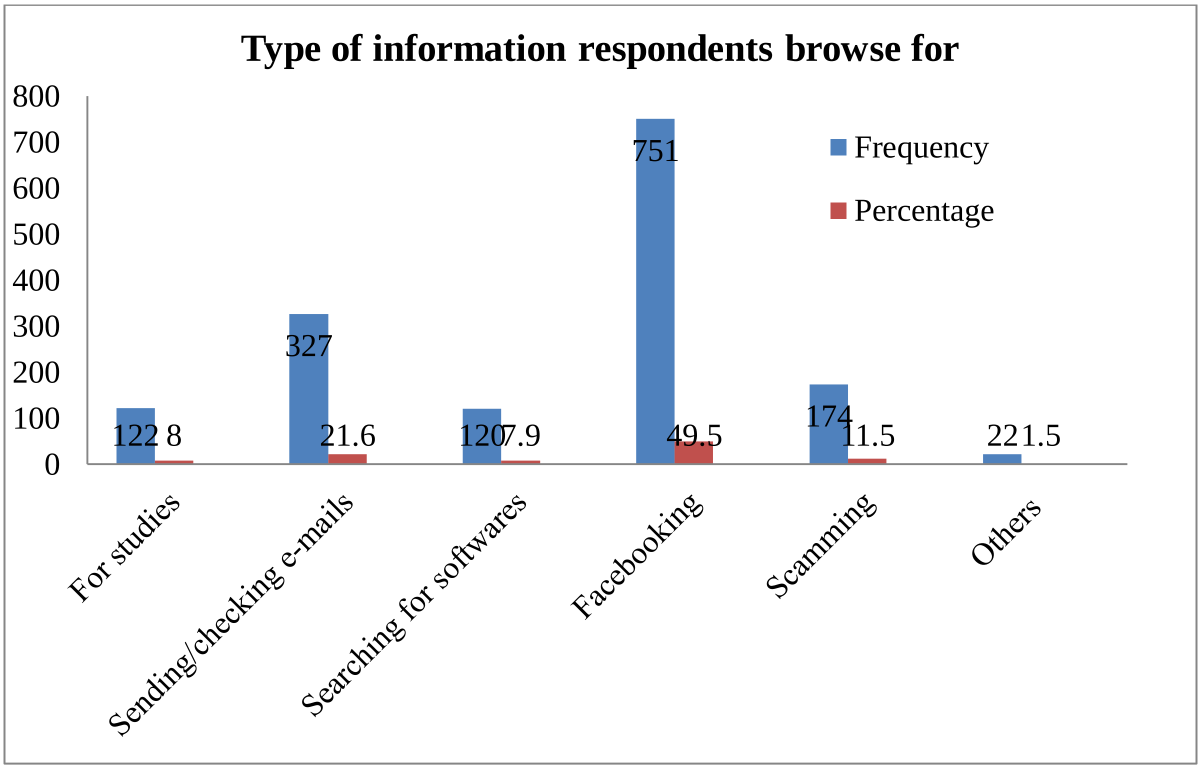


Source: Field survey, 2020

4.4.2 Type of Information Respondents Browse For

The data revealed the information presented on the Figure 4.3 below. Significant proportion of respondents 751 representing 49.5% said Facebooking. Moreover, 327 respondents representing 21.6% respondents said for sending or checking e-mails whereas 174 respondents representing 11.5% said for scamming whilst 122 respondents representing 8.0% said for studies. Again, 120 respondents representing 7.9% indicated that browse the net to searching for soft-wares and 22 respondents representing 1.5% said others.

Figure 4. 3: Type of information respondents browse for

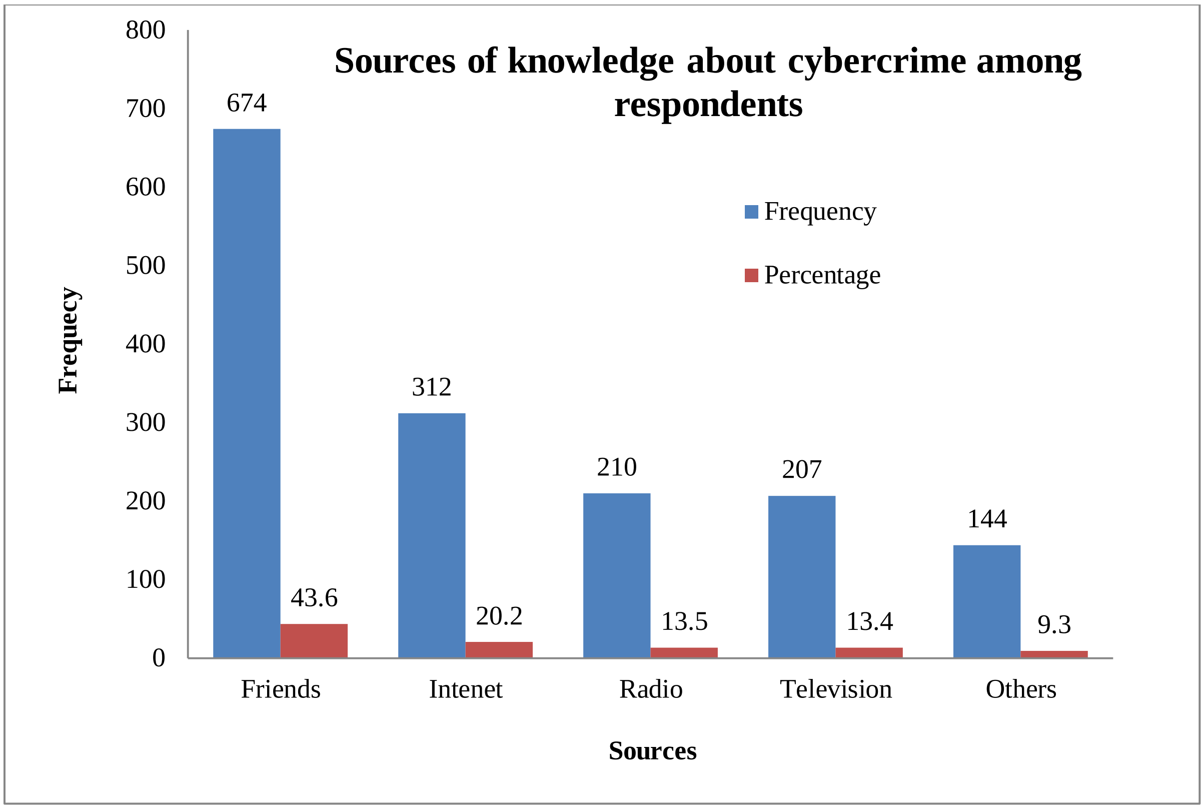


Source: Field survey, 2020

4.4.3 Sources of Knowledge about Cybercrime among Respondents

Sources from where respondents acquire their knowledge about cybercrime was also investigated and presented on the Figure 4.4 below. Respondents were asked to identify their sources of knowledge on the list of options. Majority of respondents 674 representing 43.6% acquire their knowledge about cybercrime for the first time through their friends, followed by internet 312 respondents with a percentage of 20.2%. Also, 210 representing 13.5% of respondents got to know about cybercrime through radio, whereas 207 respondents representing 13.4% gain their knowledge through television and 144 respondents representing 9.3% obtain their knowledge about cybercrime through other sources.

Figure 4. 4: Sources of knowledge about cybercrime among respondents



Source: Field survey, 2020

Respondents were further asked to indicate whether they head of cybercrime or sakawa before and 315 respondents representing 95.7% answered yes. Moreover, respondents were again asked to state whether they know anybody engaged in cybercrime or sakawa. The results showed that 322 respondents representing 97.9% said yes and 7 respondents representing 2.1% answered no. Again, respondents were asked about their engagement in cybercrime or sakawa. Greater proportion of the respondents 224 representing 68.1% said no and 105 respondents representing 31.9% said yes. Also, 316 respondents representing 96.0% think that peer influence can affect their knowledge on cybercrime and 13 respondents representing 4.0% said no.

4.4.4 Respondents Understanding of Cybercrime

Regarding the definition of cybercrime respondents were expected to define cybercrime in their opinion. This was meant to measure specific knowledge of respondents about their understanding on cybercrime. To these end 205 respondents representing 62.3% of total sampled were able to define cybercrime and remaining 124 respondents representing 37.6% had a fair knowledge in describing cybercrime.

Generally, knowledge of respondent on cybercrime was determined and classified into good, fair and poor knowledge on the table above. This was done by asking respondents to identify the type and modes of operation on cybercrime on a list they know about. This was done through the following means: Upload female pictures without their consent to deceive people online; more than half of the respondents 311 representing 94.5% percentage had good knowledge whilst 18 respondents representing 5.5% had fair knowledge (Table 4.3). Hack into people's personal and sensitive information in internet; majority of respondents 202 representing 61.4% had fair knowledge, followed by 94 respondents which represent 28.6% had poor knowledge (Table 4.3). Asking people to invest in a non-existent business on-line (Business Fraud); over half of the respondents 169 representing 51.4% had fair knowledge followed by 86 respondents representing 26.1% had good knowledge whereas 74 respondents representing 22.5% had poor knowledge (Table 4.3).

Table 4. 3: General Knowledge level of respondents on cybercrime

Mode of operation	Total	Good	Fair	Poor	Total
Upload female pictures without their consent to deceive people online	**329**	94.5%	5.5%	0%	**100**
Hack into people's personal and sensitive information in internet	**329**	10.0%	61.4%	28.6%	**100**
Asking people to invest in a non-existent business on-line (Business Fraud)	**329**	26.1%	51.4%	22.5%	**100**
Stealing a trade secret, supplier agreement, personal records, and research documents for financial gain (Industrial espionage)	**329**	70.2%	29.2%	0.6%	**100**
The use of another person's name and social security number to obtain goods and services (identity theft)	**325**	50.2%	45.3%	4.6%	**100**
The act of sending an e mail to internet users falsely claiming to be an established legitimate enterprise in an attempt to scam the users in to surrendering private information that will be used for identity theft (phishing)	**329**	28.9%	55.7%	15.4%	**100**
Practice of deceiving and manipulating investors resulting in theft of capital (investment fraud)	**327**	42.6%	55.6%	1.8%	**100**
Creation and distribution of computer viruses	**329**	36.1%	7.3%	56.6%	**100**
Cybercrime with direct contact through phone call (social engineering)	**329**	79.9%	20.1%	0%	**100**
Hacking of organizational account	**329**	46.5%	52.6%	0.9%	**100**

Source: Field survey, 2020

Stealing a trade secret, supplier agreement, personal records, and research documents for financial gain (Industrial espionage); majority of respondents 231 representing 70.2% had good knowledge, followed by 96 respondents representing 29.2% had fair knowledge and 2 respondents representing 0.6% answered poor (Table 4.3). The use of another person's name and social security number to obtain goods and services (identity theft); most of the respondents 165 representing 50.2% had good knowledge, 149 respondents representing 45.3% had fair knowledge and 15 respondents 4.6% poor knowledge (Table 4.3). The act of sending an e mail to internet users falsely claiming to be an established legitimate enterprise in an attempt to scam the users in to surrendering private information that will be used for identity theft (phishing); 181 respondents representing 55.7% had fair knowledge, 94 respondents representing 28.9% said good and 50 representing 15.4% had poor knowledge (Table 4.3).

Practice of deceiving and manipulating investors resulting in theft of capital (investment fraud); a majority 183 respondent which is 55.6% had fair knowledge, 140 respondents representing 42.6% said good and 6 respondents representing 1.8% said poor (Table 4.3). Creation and distribution of computer viruses; more than half of the respondents 185 representing 56.2% said poor, 118 respondents representing 35.9% answered good and 24 respondents which is 7.3% said fair (Table 4.3). Cybercrime with direct contact through phone call (social engineering); majority of respondents 263 representing 79.9% had good knowledge whilst 66 respondents representing 20.1% had fair knowledge and zero for poor knowledge (Table 4.3). Hacking of organisational account; more than half of respondents173 representing 52.6% had fair knowledge followed by 153 respondents which is 46.5% had good knowledge whilst 3 respondents representing 0.9% had poor knowledge. Table 3 above shows respondents' knowledge level on cybercrime (Table 4.3).

4.5 Causes of Cybercrime by Respondents

Table 4.4 confirmed by respondents that cybercrime among students is caused by the following: Pressure from, Friends, Relatives, School mates, Colleagues in my area; more than half of the respondents 169 representing 51.4% have agreed whereas 104 respondents representing 31.6% strongly agree while 51 respondents representing 15.5 were neutral and 5 respondents representing 1.5% disagreed. Get-Rich-Quick syndrome; greater majority of respondents 193 representing 59.2% strongly agreed whilst significant number 111 of respondents representing 34.0% whereas 22 respondents which is 6.7% were neutral and 3 respondents representing 0.9% did not answer. On poverty, majority 158 of respondents representing 48.0% agreed whereas 105 respondents representing 31.9% strongly agreed and 66 respondents which is 20.1% were neutral. Fame (societal recognition), 163 respondents representing 49.5% strongly agreed while 127 respondents which are 38.6% agreed whereas 39 respondents representing 11.9% were neutral. Knowledge of internet literacy; majority of respondents 153 which is 46.5% strongly agree followed by 145 respondents representing 44.1% agreed whilst 31 respondents representing 9.4% were neutral. Students see cyber fraud/sakawa as creative thinking; more than half of the respondents 198 representing 60.2% agreed whereas 73 respondents representing 22.2% strongly agreed whilst 58 representing 17.6% were neutral.

Table 4. 4: Causes of Cybercrime or Sakawa among Respondents

Causes of cybercrime	Total	Strongly agree	Agree	Neutral	Disagree	strongly disagree	Total
Pressure from, Friends, Relatives, School mates, Colleagues in my area	**329**	31.6%	51.4%	15.5%	1.5%	0%	**100**
*Get-Rich-Quick syndrome	**326**	59.2%	34.0%	6.7%	0%	0%	**100**
Poverty	**329**	31.9%	48.0%	20.1%	0%	0%	**100**
Fame (Societal Recognition)	**329**	49.5%	38.6%	11.9%	0%	0%	**100**
Knowledge of internet literacy	**329**	46.5%	44.1%	9.4%	0%	0%	**100**
Students see cyber fraud/sakawa as creative thinking	**329**	22.2%	60.2%	17.6%	0%	0%	**100**
Students see cyber fraud/sakawa as a place to deploy their knowledge	**329**	36.5%	56.5%	6.4%	0%	0.6%	**100**
Poor parenting	**329**	39.2%	50.8%	9.1%	0%	0.9%	**100**
Instant wealth is equated with smartness	**329**	40.7%	49.5%	9.7%	0%	0%	**100**
Attitude of leaders towards wealth	**329**	51.1%	35.0%	10.0%	0%	4.0%	**100**
Students see cybercrime/sakawa as a means to payback the white man for taking their forefathers as slaves and stealing resource from Africa.	**329**	73.6%	24.0%	2.4%	0%	0%	**100**
Because it is easy to practice and difficult to be identified	**329**	48.9%	43.8%	6.7%	0%	0.6%	**100**
Cybercrime victims mostly go unpunished	**329**	28.6%	50.5%	18.5%	1.8%	0.6%	**100**

Source: Field survey, 2020 ***Missing responses**

Students see cybercrime/sakawa as a place to deploy their knowledge; majority 186 respondents which represent 56.5% agreed followed by 120 respondents representing 36.5% strongly disagree. Meanwhile 21 respondents which represent 6.4% were neutral and 2 respondents representing 0.6% strongly disagreed, poor parenting; 167 respondents which represent 50.8% agreed whilst 3 respondents representing 0.9% strongly disagreed (Table 4.4). Poor parenting; majority of respondents 167 representing 50.8% agreed followed by 129 respondents representing 39.2% strongly agreed whereas 30 respondents representing 9.1% were neutral whilst 3 respondents which represent 0.9% strongly disagreed (Table 4.4). Instant wealth is equated with smartness; 163 of respondents which represent 49.5% agreed whilst 134 respondents representing 40.7% strongly agree and 32 respondents representing 9.7% were neutral (Table 4.4). Attitude of leaders towards wealth; majority 168 of respondents representing 51.1% strongly agreed whilst 115 respondents which represent 35.0% agree. However, 33 respondents representing 10.0% were neutral whereas 13 respondents which represent 4.0% strongly disagreed (Table 4.4). Students see cybercrime/sakawa as a means to payback the white man for taking their forefathers as slaves and stealing resource from Africa; more than half of the respondents 242 representing 73.6% strongly agreed followed by 79 respondents representing 24.0% agreed and 8 respondents representing 2.4% were neutral (Table 4.4). Because it is easy to practice and difficult to be identified; majority of respondents 161 representing 48.9% strongly agreed whereas 144 respondents which represent 43.8% agreed. Significant numbers of 22 respondents representing 6.7% were neutral whilst 2 respondents which represent 0.6% strongly disagreed (Table 4.4). Cybercrime victims mostly go unpunished; majority 166 respondents which represent 50.5% agreed followed by 94 respondents representing 28.6% strongly agreed whereas 61 respondents representing 18.5% were neutral whilst 2 respondents representing 0.6% strongly disagreed (Table 4.4).

4.6 Effects of Cybercrime or Sakawa on Academic Performance of Respondents

Respondents were asked to ascertain the effects of cybercrime on the academic performance of students. More than half of the respondents 294 representing 89.4% said yes, cybercrime have effects on their academic performance whereas 23 respondents representing 7.0% responded no whilst 12 respondents which is 3.6% answered no idea. Respondents were further asked to identify the nature of the effects of cybercrime on their academic performance. Majority of the respondents 295 representing 89.7% indicated negative effects whilst 28 respondents 8.5% answered positive and 6 respondents representing 1.8 said no idea.

Table 4. 5: Effects of cybercrime/sakawa on academic performance

Effects of cybercrime on academic performance	Total	Strongly agree	Agree	Neutral	Disagree	strongly disagree	Total
Poor academic performance	329	63.5%	36.5%	0%	0%	0%	100
Absenteeism	326	56.5%	49.2%	0%	0%	0%	100
Decrease ability to concentrate	329	32.6%	66.2%	0%	0%	0%	100
School dropout	329	55.9%	43.5%	0.6%	0%	0%	100
Getting arrested	328	22.5%	77.5%	0%	0%	0%	100
Going to jail	329	25.0%	74.4%	0.6%	0%	0%	100
Stigmatization	329	12.9%	85.3%	1.8%	0%	0%	100
Parental disownment	329	37.7%	62.3%	0%	0%	0%	100
Defamation of image of school	329	58.1%	36.2%	5.8%	0%	0%	100
Students who are engage in cybercrime spent more time on the internet browsing than reading/revising their books	329	18.8%	55.6%	22.5%	3.0%	0%	100
Sexual promiscuity	329	21.9%	51.7%	18.2%	8.2%	0%	100
Socially and mental harassment	329	32.6%	0.6%	14.4%	52.6%	0%	100
Students earn enough income to cater for their needs	329	59.0%	35.3%	5.8%	0%	0%	100

Source: Field survey, 2020

The data on Table 4.5 above indicates that respondents agreed that cybercrime affects students' academic performance through the following ways: poor academic performance; majority of respondents 209 which represents 63.5% strongly agree whilst 120 respondents representing 36.5% agreed to this. Absenteeism; majority of respondents 186 representing 56.5% strongly agree and 2 respondents representing 0.6% answered neutral.

Decrease ability to concentrate; more than half of the respondents 217 which represent 66.2% have agreed and 4 respondents representing 1.2% answered neutral. School dropout, 184 representing 55.9% said they are strongly agreed and 2 respondents representing 0.6% were neutral. Getting arrested by police; majority of the respondents 255 representing 77.5% have agreed and 74 respondents showing 22.5% said they have strongly agreed. Going to jail; majority 244 of respondents representing 74.4% agree and 2 respondents representing 0.6% were neutral. Stigmatisation was also identified as an effect cybercrime on academic performance of students with the following responses, majority 278 of respondents representing 85.3% agree, and 6 respondents representing 1.8% responded neutral. Parental disownment; 205 respondents representing 62.3% agree and 124 respondents representing 37.7% strongly agree. Defamation of image of school; 191 respondents which represent 58.1% strongly agree and 19 respondents which represents 5.8% neutral. Students who are engage in cybercrime spent more time on the internet browsing than reading/ revising their books; 183 respondents representing 55.6% agree and 10 respondents representing 3.0% disagree. Sexual promiscuity; 170 respondents which represent 51.7% agree and 27 respondents which represents 8.2% disagree. Socially and mental harassment; majority 172 respondents representing 52.6%

disagreed, followed by 106 respondents which is 32.4% strongly agree, 47 respondents representing 14.4% were neutral and 2 respondents which represents 0.6% agreed. Students earn enough income to cater for their needs, more than half of the respondents 194 representing 59.0% strongly agree and 19 (5.8%) neutral.

Table 4. 6: Relationship between some demographic characteristics of respondents and involvement in cybercrime

Demographic characteristics of respondents	Correlation coefficient	P value	Definition
Level/form of respondent	0.267**	0.000	Positive correlation
Gender of respondents	0.119*	0.031	Positive correlation

Source: Field survey, 2020

From the Table 4.6 above, it is revealed that there is a positive relationship between the level/ form and gender status of respondents and their' involvement in cyber-crime with p values, $p < 0.001$ and $p < 0.05$, respectively. Thus, the relationship between the level/ form and gender statuses of respondents and their involvement in cyber-crime is invariable. This implies that the more a student is higher in terms of form/level in education the more he is likely to be involved in cybercrime and the lesser academic level they find themselves, the lesser they are involved in cyber-crime. Likewise, as revealed in the Table 4.6 above, the more the male respondents, the more likelihood that they would be engaged in cyber-crime and the lesser males of respondents, the less likelihood that they would be involved in cyber-crime.

CHAPTER FIVE

DISCUSSION

5.1 Introduction

This chapter of the thesis discusses the major findings of the study in relative to previously published data and evidence. Findings from qualitative study were triangulated with quantitative results and presented.

5.2 Socio-Demographic Characteristics

Majority of respondents were males, few were females. This skewed proportion of sex toward male could be ascribed to the fact that Vitting Senior High is a technical school. However, this finding is in line with Warner (2011) who reported that most Ghanaians involved in cybercrime are males. Also, the Attorney General's Department of Australia (AGDoA, 2013) testified that most of victims involved in cybercrime are males. Okeshola and Adeta (2013) and Adedayo (2008) also confirmed that cybercrime is for male youth in Nigeria.

The age distribution indicates that half of the respondents who participated in the survey, were between the age bracket of 16 - 18 years. This complies with the Ghana education service regulations where the admission point to Senior High School fifteen to sixteen years. A good number of the respondents have both parents' lives. The results also indicates that a little above half of the respondent parents are married. The results again indicate that getting to half of the respondents' parents never had any formal education.

The level/form of respondents were also categorised into SHS 1-3 with the greatest percentage of respondents representing 39.5% were in year two. With regards to residential status of respondents majority are residing in the boarding house.

5.3 Perceived Prevalence of Cybercrime among Students

In assessing how respondents perceived the prevalence of cybercrime among senior high students of Vitting Senior High, the study discovered that majority of students indicated that cybercrime is a very common practice among secondary school students whereas few of them stated that cyber-crime is not a common practice. Likewise, the key informants (Assistant head master and senior house master) also established that the prevalence of cyber-crime is very common. This is similar to the findings of Chinasa and Odo (2017) and Odumesi (2014) who found that students' involvement in cybercrime activities is very common in school. However, it must be noted that their studies were carried out in tertiary institutions. In an attempt to really describe how prevalent cyber-crime is in Vitting SHS below is what the senior house master said.

> *"It is here, it has been here and it is still there. Most students are involved in it and the popular one they do is the sakawa, we also call them game boys. Yes, they do it a lot and a good number of students are into it and they are able to do it both internally and externally".*

Further, the senior house master said this to validate his claims:

> *"Because I am the senior house master, I visit the student dormitories very frequently so, one faithful day, my dormitory visits during prep hours afforded me a chance seize a mobile phone from student who did not go for preps. Upon going through the phone, I saw a lot of beautiful female pictures and other fake receipts*

> *so I decided to call him to open up on is deeds otherwise he would not get the phone so he opened up and confessed to me. Now that is what he does to take care of himself in the school, scamming".*

In addition, this is what the senior house master had to say to indicate how common cyber-crime is on the Vitting campus

> *"During our Parents Teachers Association meeting they confirmed that they were duped by students am sure these are all cybercrimes aside the popular sakawa we all know".*

It would not be out of place therefore to state that cybercriminals can be found in any institution both in secondary and tertiary schools subject to their degree of exposure to technology.

5.4 Prevailing Practices

From the data obtained majority of respondents agreed that the most prevalent cybercrime practice among students is deceiving and manipulation of investors resulting in stealing of capital through fake documentation as the most common cybercrime practice, validating the results as stated by the head master and the senior house master that students fake documents a lot to deceive people. The key informants were of the view that within the school they had issues of students falsifying documents such as results, lying to parents for money either for hospitals, fees, and buying books and so on and so forth. Below is a narration by the Senior house master on the practice of falsification of documents:

> *"Just recently we had a case like that, a student came for a testimonial, he came with an internet print out of his West African Senior School Certificate Examination (WASSE) results so we looked at it and said no we don't accept it he should go and bring the original certificate, however we have taken the print out when he came we realized he had altered the grades. The results looked different than what was on cert, so I think this are all examples of cybercrime".*

This finding contradicts Adedayo (2008) who found that students use of another person‘s name and social security number to obtain goods and services (identity theft) are the most common internet crime among students. The results further indicated that almost half of respondents strongly agreed that students sent e-mails to impersonate credible institutions to steal personal or financial information via a contaminated link. Whereas almost half of also agreed that students use credit card of other people illegally to buy goods and services online. More than half of respondents agreed that students do send email to internet users portraying themselves as legitimate business owners to scam users into giving out private information that will be used for identity theft.

Again, majority of respondents agreed that students buy goods and services online without paying. These findings are in line with Adedayo (2008) studies about Secondary School Students' awareness of rates of internet crimes. Further findings revealed that 41.9% respondents agreed to the fact that students persuade people to invest in a non-existent business on the internet, example gold. This agrees with Warner (2011) that identified fake gold scam committed in Ghana as a form of cyber scam. As, students believed that Ghana is recognised for its richness in gold, they are able to influence foreigners on deals about gold mining companies based in Ghana. Warner (2011) affirmed that to allay the fear of these foreigners, the criminals' forged documents to support every claim they make. Majority of the respondents strongly agreed and agreed that students also use dating sites to deceive and manipulate people resulting in stealing of capital. This finding corroborate with studies by Whitty and Buchanan (2012) and Warner (2011) that online dating otherwise known as romance scam is popular where prime targets are older, divorced or widowed white women. In this regards culprits fraudulently initiate a relationship through online dating sites then dupe their targets of huge sums of money through false gifts and air tickets for visits. Cyber-crime is very common in this school, claimed by both Assistant headmaster in charge of academics and the senior house master. Students according to the senior housemaster were easily seen involved in this internet crime to the extent that during P.T.A meetings some of these issues are been brought up for discussing. Below is what the assistant head, academics had to say regarding the prevalence of cyber-crime in Vitting S.H.S.

> *"Sakawa if you like cybercrime is prevalent here both in the open and hidden and sometimes we do receive complaints from parents. What I meant by both open and hidden is that some of the students practice it openly with pride and they declare themselves as "shatters or game boys". They are mostly from final year students and few from form two. The hidden ones hide their identities. They don't want to be known or seen by their colleague students or teachers that they have any form of association with scamming. So they hide to practice it".*

5.5 Knowledge Level of Respondents on Cybercrime

Singh and Bala (2014) revealed that internet plays significant roles in the life of students making it much easier for them to search for vital information which will improve their level of comprehension, reading skills and their academic performance. However, if this is left unsupervised could lead students to internet crime. In respect this; opinions of respondents were sought on their access or use of internet. The study revealed that nearly all of respondents said they have been using internet. This study conforms to Martis (2018) and Okeshola and Adeta (2013) results of 99.7% and 99%, respectively on access and usage of internet by students in India and Nigeria respectively. By this we can conclude that nearly all the respondents use the internet for one activity or the other. More than half of respondents said yes they have e-mail/ Facebook accounts. Almost half of the respondents use the internet for Facebooking. This result contradicts with Islam (2018) studies who found majority of students browse the internet mainly for studies. However, Obiri Yeboah (2015) who disclosed that internet and access to technology lead secondary school students to browse Facebook making them vulnerable to many forms of internet crimes instead of studies to better lives for future.

The study further examined the knowledge of respondents on cybercrime by asking specific question. Respondents were asked whether they head of cybercrime or sakawa before and nearly all of respondents answered yes. This is similar to Okeshola and Adeta (2013) findings where majority of respondents (94%) answered that they have head of cybercrime before. Further probes were made to identify their sources of knowledge. Few of the respondents acquired their knowledge about cybercrime, for the first time through their friends. Data from Adejoh *et al.* (2019) also found similar results that many young people of school going age are initiated in cybercrime through their peers called yahoo boys and girls. This is because they want be like them living in an extravagant and flashy lifestyle. This is also in line with Amosun and Ige (2009) who found that more than halve of students involved in cybercrime learnt it from their peers either in the same school or from other schools. This comply with the Differential Association Theory (DAT), Sutherland (1939) criminal behaviour is learned in the same manner as law-abiding values are learned through peers within intimate groups. Again, internet was also identified as another source of knowledge, radio, television and through other sources. The closeness of the percentages indicates that various sources teach students how to do cybercrime or sakawa.

To measure specific knowledge of respondents on cybercrime, precise questions on cybercrime were asked for respondents to answer in order to confirm their knowledge level. Respondents were asked to state whether they know anybody engaged in cybercrime or sakawa and nearly all of respondents said yes. Again, respondents were asked about their engagement in cybercrime or sakawa and majority of the respondents said no. Whilst nearly all the respondents think that peer influence can affect their knowledge on cybercrime.

5.6 Respondents Understanding of cybercrime

Majority respondents were able to defined or described cybercrime to capture some key terms about cybercrime as “internet and computers”. “They defined cybercrime as crime which is committed through the internet either by a phone or computer.” This similar to Hassan *et al.* (2012) definition on cybercrimes as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victims directly or indirectly, using modern telecommunication networks aided by computers and mobile phones. Few had a fair knowledge in describing cybercrime. The respondents' ability to define cybercrime further confirmed an appreciable accepted level of their knowledge in cybercrime.

This is how Assistant headmaster in charge of academic affairs defined cybercrime or sakawa;

> *"It is any form of fraudulent activities or transactions either by means of sales or exchange using computers through the internet or cyber space. This kind of crime can be committed everywhere one can have access to the internet and computers, examples cyber cafes, your house, class room, dormitories, in your car etc.".*

Senior house master also define cybercrime or sakawa as;

> *"In my opinion it has to do with a situation where people or individuals take advantage of globalisation, as a result of easy internet access to commit crime i.e. extortion of money (sakawa) from people from other jurisdictions and even within the country".*

However, the senior house master was quick to add that it is not only limited to sakawa but also, it has to do with falsification of documents where people are able to alter certificates or results slip on the internet for their personal gains. Below is what the senior house master had to say about that:

> *"Just recently we had a case like that in this school where a student came for testimonial, he came with an internet print out so we looked at it and say no we don't accept it he should go and bring the original certificate, however we have*

> *taken the print out when he came we realised he had altered the grades that was not what was on cert, so I think this are all examples of cybercrime*".

Data also indicated that respondents have good and fair knowledge about the type and modes of operation on cybercrime in which students are involved into. Nearly all the respondents had good knowledge on, upload female pictures without their consent to deceive people, hack into people's personal and sensitive information in internet. Majority of the respondents had fair knowledge. Asking people to invest in a non-existent business on-line (Business Fraud); majority of the respondents had fair knowledge. Stealing of trade secret, supplier agreement, personal records, and research documents for financial gain (Industrial espionage); more than half of respondents had good knowledge. The use of another person's name and social security number to obtain goods and services (identity theft); most of the respondents had good knowledge. The act of sending an e-mail to internet users falsely claiming to be an established legitimate enterprise in an attempt to scam the users in to surrendering private information that will be used for identity theft (phishing); majority of respondents had fair knowledge in this act. Practice of deceiving and manipulating investors resulting in theft of capital (investment fraud); majority had fair knowledge. Cybercrime with direct contact through phone call (social engineering); majority of respondents had good knowledge. Hacking of organisational account; more than half of the respondents had fair knowledge. These findings corroborate with studies by Amini-Philips (2018) where he discovered a very high level of knowledge mean of students which is greater than his criterion mean value of 2.50. Also, Ben (2017) studies on undergraduate students' knowledge level also prove high (90%) score. However, in terms of creation and distribution of computer viruses; more than half of the respondents said they have poor knowledge about it. This is in conformity with Martis (2018) that found that students' youth are generally lacking the knowledge concerning cybercrime hence their personal computers and laptops are been attacked by viruses which are distributed by cyber criminals. Finding from both qualitative and quantitative data revealed that students have knowledge in cybercrime or sakawa.

Regarding the knowledge of the activities of cybercrime and other procedures involved in scamming innocent preys, the key informants confirmed students' awareness and knowledge of the phenomenon. The key informant (Assistant headmaster, academics) explains:

> *"Cybercrime or sakawa comes in different formats ranging from romance scam, identity theft, credit card theft, direct phone calls, e-mail phishing and so on. But what is come among the student is romance scam where old foreign wealthy widows and single are lure and deceived into a romantic relationships in order to get financial gains and other remunerations".*

5.7 Causes of Cyber Crime

In this part, efforts are made to investigate the causes and inspiring elements which drive Senior High School students to cybercrime or sakawa practice. Pressure from friends, school mates and colleagues in my area; more than half of the respondents have agreed to this and poverty. These two conforms to Okeshola and Adeta (2013) findings on the nature, causes and consequences of cybercrime in tertiary institutions in Nigeria. They concluded that 87% were of the opinion that poverty is a major cause whilst 86% of the respondents admitted that peer group is the cause of cybercrime in Nigeria tertiary institutions. Universally, poverty appears to be places where is crime. Confirmation provided by Meke (2012) shown that, poor people are more into cybercrime than the rich people.

Other causes identified includes, Get-Rich-Quick syndrome; majority of respondents strongly agreed. Fame (societal recognition) and knowledge of internet literacy almost half of respondents strongly agreed. Obiri Yeboah (2015) agreed with 55% confirmation that get rich quick and societal recognition (fame) are some of the factors that pushed youth into cybercrime. People what to start making money as soon as possible forgetting the approved means to riches. Students see cyber fraud/ sakawa as creative thinking and cybercrime/sakawa as a place to deploy their knowledge, more than half of the respondents agreed. These two agrees with Dashora (2011) findings that most school children involvement in computer crime emanates from curiosity and inquisitives to know. Students want to be creative thinkers and always want demonstrate that they are the best amongst their colleagues.

Poor parenting, half of the respondents agreed. Parenting is very important in guiding and shaping children through the right direction. Where there is poor parenting children adopt some life styles which do not conform to societal norms and good morals which often lead children to delinquencies. This confirm the central theme of Merton’s social theory that societal structures could lead (pull and/or push) people into social vices like crime. Okeshola and Adeta (2013) concluded that 85% of cybercriminals are generally young or youth who may be exposed to the internet earlier without proper parenting. Instant wealth is equated with smartness; almost half of the respondents agreed. Attitude of leaders towards wealth, majority of respondents strongly agreed. Students see cybercrime/

sakawa as a means to payback the white man for taking their forefathers as slaves and stealing resource from Africa; more than half of the respondents strongly agreed. Majority of respondents representing strongly agreed that it is easy to practice and difficult to be identified. Majority of the respondents agreed that cybercrime victims mostly go unpunished. These compliment findings of Okeshola and Adeta (2013) that declared that factors that inspire young people into cybercrime vary based on multiple reasons such as monetary gains, fame, easy to escape from conviction due to weak law enforcement, easy to execute, vengeance and to be recognised as smart and intelligent.

The qualitative data gives clear clarifications on the causes of cybercrime or sakawa. No one is island. People mingle and associate themselves for many reasons. People influence each other especially the youth to involve in deeds which are both positive and negative. Peer group influence cannot be over emphasized as articulated by the assistant headmasters, academics. He further narrated that:

> *"The motivating factors vary Peer group influence. Most students are pushed into sakawa because of their friends. They want fit in well with their peers and so they must do what their friends are doing. "They say show me your friend and I will tell you your character".*

Parents are regarded as agents of socialisation. They are expected to guide, nature and teach their children good standards and morals which conforms with the societal norms and ethics. However, for love of money and other reasons most parents are departed from their parental roles and responsibilities as further explained by assistant head, academics:

> "*Also, to the household level I think that it could be caused by poor parenting or lack of it. Some parents don't care about their children. What they do, who they*

> *move with, where they are and even where they sleep they just don't care. Some parents even support their children in committing crimes. Other causes are get-rich quick syndrome, pleasure, poverty fame and recognition, access to technology e.g. smart phones and other hand held gadgets can be used to perpetrate cybercrime. Internet or computer literacy; some of them want to test what they know about computer and internet and they end up been shatters. Most of them think that they are taking back what was stolen from their forefathers by the white man through colonisation and slavery. This is some form vengeance".*

The senior house master agreed with the opinion communicated above. According to him the causes of cyber-crime are numerous and dependent upon the upbringing and the environment in which the criminal grew up. Nevertheless, according to him (senior housemaster) some of the causes included peer pressure, poverty, ignorance, poor parental care etc. Below in the narration is what the senior housemaster had to say regarding how pressure from peers can be a cause of cyber-crime:

> "*You know, these criminals sometimes make huge monies from their dubious acts, and when this is the case, thus when these cyber-criminals colleagues' see or realize they have gotten ABCD as a result of their engagement in cybercrime, they easily become motivated and influenced into doing same in order to get the wealth and assets their friends also have. Birds of the same feather flock together. Over 50% of students that are into sakawa because peer influence".*

From the above, it can be deduced from both quantitative and qualitative data that peer pressure, the quest for quick, poverty, fame, internet literacy, intellectual pursuit, poor parenting, instant wealth is equated to smartness, attitude of leaders towards wealth, vengeance or payback, easy to practice and low chance of being trapped and indicted as results of loose laws are the inspiring causes for persons involvement in cybercrime. These factors identified and discussed above further to endorse the central theme of Merton's social strain theory that societal structures could lure people into social vices like crime.

5.8 Effects of Cybercrime or Sakawa on Academic Performance of Respondents

Cybercrime is an issue of public concern as it has implication on students' academic progress and the entire society at large. The study showed more than half of the respondents said yes cybercrime have effects on their academic performance. This strongly contradicts with Denga (2011) finding which concludes that students are entirely occupied and engaged with academic and vocational programmes that can make them independent and better future leaders. A further probe to identify the nature of the effects of cybercrime on their academic performance revealed that majority of the respondents indicated that the nature of effect of cybercrime is negative. This is in line with Okeshola and Adeta (2013) studies where over 90% of respondents answered that cybercrime have negative effects in general performance of students.

The analysis from the data further indicates that respondents agreed that cybercrime affects Senior High School academic performance through the following ways: poor academic performance; majority of respondents strongly agree and agreed. On absenteeism majority of the respondents strongly agreed. Decrease ability to concentrate; more than half of the respondents have agreed. On school dropout, majority of the respondents said they are strongly agreed. This means that students who are involved in this business can turn to be an absentee which could lead to poor academic performance as they missed important lessons and also decreased the concentration in general and eventually lead them to quit schooling. Reports in our dailies corroborate to the fact that cybercrime threatens the educational progress of children under school going age in Ghana. School children often leave the classroom for internet cafés in order to be involved in the act. This affects academic progress as those involved fail to attend school for a considerable period of time (Ghana news agency, 2017).

Getting arrested by police; majority of the respondents have agreed. Going to jail; more than half of respondents have agreed. Stigmatisation was also identified as an effect cybercrime on academic performance of students with the following responses, majority agreed. Parental disownment, majority of the respondents agreed. Defamation of image of school; more than half of respondents strongly agreed. Students who are engage in cybercrime spent more time on the internet browsing than reading/ revising their books; representing majority have agreed, Sexual promiscuity; more than half agreed, Socially and mental harassment; majority of respondents disagreed. Student earn enough income to cater for their needs, majority of the respondents strongly agreed.

As narrated by the assistant head, academics through an in-depth interview, worst things have negative effects. This sakawa thing can damage the image of this school and even Ghana at large. I understand currently Ghana is been listed among top ten countries where cybercrime is most prevalent and third in Africa. This can scare foreign investors away from the country as a result of this bad image. To support his claim he explained that:

> *"Mmmmh! one day they called to tell me that one of our past student was arrested by police for involving in sakawa, this can tarnish the image of the school. School*

> *dropout is another effect. Most of them stop schooling in order to concentrate on this fraudulent business of making money through sakawa. Other effects are poor academic performance, absenteeism, decrease ability to concentrate, socially and mental harassment, stigmatisation, getting arrested, spiritualism, death and so on".*

Senior house master also has this to say from the interview. It was revealed that the effects of cyber-crime are obvious and negative in any circumstance. According to the senior house master, the effects of cyber-crime could range from poor academic performance, truncated education, to death especially those of the criminals who have taken cyber-crime to the extreme. Below is what the senior house master said about the effect of cyber-crime on academic performance;

> *"My friend, those engaged in cyber-crime don't have time for their studies, they don't have time for their books. They always concentrate on their phones browsing here and there and as a result of that those who are not lucky and caught, they are punished, we suspend them, make them day students. Some are given several days punishment on campus and all these will take them away from books so it will lead to poor performance".*

CHAPTER SIX

SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.0 Introduction

This study was pursued to assessing the effects of cybercrime on senior high school students of Vitting Senior High School in the Tamale Metropolis. The study centered on the prevalence of cybercrime among the students, knowledge level of students on cybercrime in the school, to identify causes and effects of cybercrime on academic performance of students.

6.1 Summary of Findings

Analysis of the socio-demographic characteristics of the respondents shows 76.9% were males whilst 23.1% were females. The age distribution indicates that a good number of the respondents were between the age brackets of 16 – 18 years. Getting to half of respondents 41.0% lives with both parents and 50.2% of the respondent parents or guardians are married. The results again indicates that majority of respondents' parents 146 representing (44.4%) never had any formal education. The greatest percentage of respondents 39.5% were in year two and 79.6%) out of the total respondents are residing in the boarding house.

The study revealed that majority of students 81.2% indicated that cybercrime is a very common practice among secondary school students whereas. Likewise, the key informants (Assistant head master and senior house master) also established that the prevalence of cyber-crime is very common and prevalent among students of Vitting Senior High Secondary School. The study also found that majority of respondents representing 67.5% agreed that the most prevalent cybercrime practice among students is deceiving and manipulation of investors resulting in stealing of capital through fake documentation as the common cybercrime practice. This was validated the key informants that within the school they had issues of students falsifying documents such as results, lying to parents for money either for hospitals, fees, and buying books and so on and so forth. Below is a narration by the assistant head master on the practice of falsification of documents:

> *"Just recently we had a case like that, a student came for a testimonial, he came with an internet print out so we looked at it and said no we don't accept it he should go and bring the original certificate, however we have taken the print out when he came we realized he had altered the grades that was not what was on cert, so I think this are all examples of cybercrime".*

The study showed that 95.7% respondents have been using the internet. More than half of respondents 84.8% said yes they have e-mail/Facebook accounts, 41.0% said they browse for studies. The study further indicated that 95.7% of respondents' have head of cybercrime before and few of them 20.9% acquires their knowledge about cybercrime through their friends. 62.3% had good knowledge about cybercrime or sakawa.

Students had good knowledge on the following cybercrime practices; Cybercrime with direct contact through phone call (social engineering) representing 79.9%, upload female pictures without their consent to deceive people online 61.4%, hack into people's personal and sensitive information in internet 61%. Asking people to invest in a non-existent business on-line (Business Fraud) 51.4% followed by the use of another person's name and social security number to obtain goods and services (identity theft) representing 50.2%.

The study deduced from both quantitative and qualitative data that peer pressure, vengeance or payback 73.6%, the quest for quick riches 58.7%, poor parenting 50.8%, fame 49.5%, easy to practice and low chance of being caught 48.9%, poverty 48%, internet literacy 46.5%, are the inspiring causes for students' involvement in cybercrime. The results of the study also shows that 89.4% respondents said yes cybercrime have effects on their academic performance. Majority 89.7% indicated that the nature of effect of cybercrime is negative.

The study found out that cybercrime affects Senior High School academic performance through the following ways: getting arrested by police 77.5%, going to jail 74.4%, decrease ability to concentrate 66.2%, poor academic performance 63.5%, absenteeism 56.5% and school dropout 55.9%.

6.2 Conclusion

The study found that based on the perceptions of student's cybercrime is prevalent and very common among senior high school students. A good number of students are into it practices both internally and externally. Many of the respondents were knowledgeable in cybercrime. Majority of them were able to identify modes and operations of cybercrime and their source of knowledge were indicated as friends, internet, radio and television. Therefore, education in any form whether formal or non-formal can be regarded as a good source of knowledge.

The study revealed that most students who engaged in cybercrime are from form 3, however only few of them came from form 2 and 1.

The study revealed that respondents identified peer pressure, vengeance or payback, the quest for quick riches, poor parenting, fame, easy to practice and low chance of being caught, poverty, Internet literacy as the major inspiring causes for students' involvement in cybercrime.

It appears from the study that students engagement in cybercrime had negative effects on their academic performance. Therefore, students involvement in cybercrime led to decline in their academic performances.

It came out of the study that getting arrested by police, going to jail, decrease ability to concentrate, poor academic performance, absenteeism and school dropout were some of the effects connected with cybercrime among students.

6.3 Recommendations

Cybercrime for the past years is considered as a worldwide phenomenon affecting almost individuals and nations and most countries consider it fight as a major priority. In view of this the following recommendations could be a great influence in the fight against cybercrime to either prevent or bring it down to a barest minimum among the youth especially senior high school.

The results from the study indicated that students perceived cybercrime to be very prevalent and common among students and a good number of students are into it practices in secondary school. The study however, recommends that the secondary schools' curriculum must include courses on cybercrime to manage and educate students on the effect of cybercrimes on their studies.

National Cyber Security Awareness Program (NCSAP) should endeavour to sponsor media (internet, radio and television) to strengthen and intensify education through awareness creation in order to have cybercrime free society since these are the students' common source of knowledge on cybercrime with focus on the youth which includes senior high students. This can educate the public on the act, effects and other consequences of cybercrime to every citizen found anywhere in the community, school, mosques, churches and homes.

The school authority should collaborate with parents to counsel and educate students on the effects on their engagement in cybercrime on their academic performance. The school can establish guidance and counseling unit in the school to give counseling to culprits within the school in various forms and also teach them morals.

Considering the diverse nature of the cause of cybercrime it require a collective approach between appropriate Ghanaian authorities and the citizenry in order to help fight this menace. The justice system must come out with policies to deal with all matters relating to cybercrimes by establishment of cybercrime courts in the country to prosecute cybercriminals and parents who do not take good care of their children by allowing them engage is such crime. They should also encourage more people to take up courses on cyber law and cybersecurity in a form of scholarship especially lawyers and judges within the justice system.

Cybercrime is a worldwide canker which needs collaboration to deal with. Therefore, it needs intelligence and other best practices from countries that are able to chalk success in the fight against this crime such as United States of America, France, and Britain. Some of these cybercriminals acquire computer technologies from these countries to perpetuate such crimes. Therefore, cooperating with them can motivate them to effectively assist in fighting this crime by blocking the sources they acquire those sophisticated computer software and technologies.

The Ghana Police Service is not well resource in terms of training and tools to fight cybercrime in the country. This is why cybercrime is easy to practice with low chance of being caught. This therefore calls for improve training programmes with more concentration on ICT skills development. This will be equipped them with the knowledge to deal with different categories of cybercrime.

REFERENCES

Abem, E. C. (2013). *Combating cybercrime in Ghana: prospects and challenges.* (Doctoral thesis, University of Ghana). Published.

Abugri, S. (2011) Ghana: Internet criminals cashing in on e-waste. *New African*. Retrieved from: http://www.sydneyabugri.com/Home2/features/217ghana-Internet-criminalscash-in-on-e- waste-dumping.html. Accessed on 25/02/2019.

Abotchie, C. (2012). *Treatment of criminals and crime prevention in Ghana*. Accra: Hans Publications.

Adedayo, 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*.

Adeleke, R. G. (2017). *Perception of cybercrime among Nigerian Youths, A Case Study of Caritas University*. *Pp. 5- 47*. Retrieved from: https://uniprojects.net/project_materials/perception-of-cybercrime-among-nigerian-youths/Retrieved on 2/11/2019

Adejoh, S. O., Alabi, T. A., Adisa, W. B., & Emezie, N. M. (2019). "Yahoo boys" phenomenon in Lagos metropolis: A qualitative investigation. *International Journal of Cyber Criminology*, *13*(1), 1–20.

Aiken, M., Davidson, J., & Amann, P. (2016). *Youth pathways into cybercrime.* Paladin Capital Group.

Akuta, E. A., Ong'oa, I. M., & Jones, C. R. (2011). Combating cybercrime in Sub-SaharaAfrica; a discourse on law, policy and practice. *Journal of Research in Peace, Gender and Development*, *1*(4), 129 – 137.

Alkaabi, A., O., S. (2010). *Combating computer crime: an international perspective,* (Doctoral Thesis on Information Security Institute, Faculty of Science and Technology, Queensland University of Technology).

Amini-Philips, C. (2018). Awareness and Involvement in Cybercrime among Undergraduate Students in Universities In Rivers State, Nigeria. *International Journal of Humanities and Social Science Invention, 7*(03).

Amosun, P. A., & Ige, O. A. (2009). *Internet crime: A new breed of crime among in-school aged children in Nigeria.* In The African Symposium (p. 90).

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, *22*(2), 171-192.

Ani, L. (2011). Cybercrime and national security: the role of the penal and procedural law. *Law and Security in Nigeria*, 200-202.

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

Attorney General's Department of Australia. (2013). *National Plan to Combat Cybercrime. Commonwealth of Australia.* Retrieved from: http://www.ag.gov.au/. on 23/03/2019.

Barfi, K. A., Nyagorme, P., & Yeboah, N. (2018). The internet users and cybercrime in ghana: evidence from senior high school in Brong Ahafo Region. *Library Philosophy and Practice,* 1-16.

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

Bjarnason, T., & Adalbjarnardottir, S. (2000). Anonymity and confidentiality in school surveys on alcohol, tobacco, and cannabis use. *Journal of Drug Issues*, *30*(2), 335-343.

Boateng, R. (2014). *Research made essay*. Accra: PearlRichards Foundation.

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. (2010). *Cybercrime and criminality in Ghana: its forms and implications*. In AMCIS (p. 507).

Brenner, S. W. (2010). *Cybercrime: criminal threat from cyberspace.* Santa Barbara, CA: Praeger.

Britz, M. T. (2008). *Computer forensics and cybercrime: an introduction*. Upper Saddle River, NJ: Prentice Hall.

Brody, R. G., & Perri, F. S. (2016). Fraud detection suicide: the dark side of white-collar crime. *Journal of Financial Crime*.

Burns, N., Grove, S. K., & Stuppy, D. J. (1993). The practice of nursing research: Conduct and utilization.

Burrell, J. (2008). Problematic employment: West African internet scams as a strategic misrepresentation. *The MIT Press*, *4*(4), 15-30.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36-54.

Centre for Strategic and International Studies (2013): The impact of cybercrime and cyber espionage. Retrieved from: www.csis.org on 25/02/2020.

Correa, D. (2016). Costs of talktalk breach amount to £60m. *SC Magazine UK*. Retrieved from: http://www.scmagazineuk.com/costs-of-talktalk-breach amount-to 60m/article/470968/ on 22/09/2019.

Council of Europe Convention on Cybercrime (2010). Access from https://www.coe.int/en/web/conventions/ on 25/03/2020

Creswell, J. W. (2013). *Research design: qualitative, quantitative, and mixed methods approaches*, 3rd ed. Los Angeles, Sage publications.

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. SAGE publications.

Daniel, E. (2015). *Cybercrime in Ghana A Study of Offenders, Victims and the Law* (Doctoral dissertation, University of Ghana).

Dashora, K. (2011). Cybercrime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences*, *3*(1), 240-259.

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

De Vaus, D. (2002). *Analyzing social science data: 50 key problems in data analysis*. sage.

Walliman, N. (2015). *Social research methods: The essentials*. Sage.

Dictionary, M. W. (2002). Merriam-webster. Retrieved from: *On-line at https://www.merriam- webster.com/dictionary/malware* on 25/03/2019.

Elmes, D., Kantowitz, B., & Roediger III, H. (2011). *Research methods in psychology*. Cengage Learning.

Federal Republic of Nigeria (FRN, 2013). "*National strategy on education*," 5th edition, Lagos: NERDC press.

Ghana News Agencies (2017). Education in Ghana: Students failing BECE Because of sakawa and Porn – GES Director. Retrieved from: http://ghheadlines.com/agency/pulse/20170529/44309306/education-in-ghana-students-failing-bece-because-of-sakawa-and-porn-ges-director on 28/09/2019

Ghana News Agency. (2009). Ghana to set up cybercrime response team. Retrieved from: http://ghanabusinessnews.com/2009/08/19/ghana-to-set-up-cyber-crime-response-team/ on 29/09/2019

Ghana National Cyber Security Policy & Strategy (2014) Report. *Republic of Ghana, Ministry of Communications,* Ghana.

Ghanaweb.com (2015). 2 Ghanaians arrested in US over credit card fraud. Retrieved from https://www.ghanaweb.com/GhanaHomePage/NewsArchive/2-Ghanaians-arrested-in-US-over-credit-card-fraud-379539 on 29/09/2019

Global Complex Innovation (2014). Access from: https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors on 25/03/2020

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

Graphic.com.gh (2018).Victims lose $95m to cybercrime. Retrived from: https://www.graphic.com.gh/news/general-news/ghana-news-victims-lose-95m-to-cybercrime.html on 29/09/2019

Graphic online (2017). Credit Card Fraud: What you need to know. Retrieved from: https://www.graphic.com.gh/business/business-news/credit-card-fraud-what-you-need-to-know.html on 29/09/2019

Hakim, C. (2000). *Research design: Successful designs for social and economic research,* 2nd ed. New York, Routledge

Halder, D., & Aishankar, K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global.

Harris, L. (2015). Rise in child and teen fraud arrests mainly due to increase of internet-based crimes. *Daily Telegraph*. Retrieved from: http://www.dailytelegraph.com.au/news/nsw/rise-in-child-and-teen-fraud-arrests-mainly-due-to-increase-ofinternetbased-crimes/news story/fc620acdb8379e30ab46f17493e40475 on 22/09/2019.

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

Hilbert, R. A. (1989). Durkheim and Merton on anomie: An unexplored contrast and its derivatives. *Social Problems*, *36*(3), 242-250.

Igba, I. D., Igba, E. C., & Nwambam, A. S. (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement. *International Journal of Applied Engineering Research*, *13*(2), 1144-1154.

Ige, O. A. (2008). Secondary school students' perceptions of incidences of Internet crimes among school age children in Oyo and Ondo States, Nigeria. *A Master dissertation in the Department of Teacher Education, University of Ibadan*.

Internet Crime Complaint Center (IC3) (2018) Annual Report. Retrieved from https://cybersecurityventures.com/fbi-releases-ic3-2017-internet-crime-report-calls-for-increased-public-awareness/ on 29/03/2019

Internet Crime Complaint Center (IC3) 2008 Annual Report. Retrieved from https://www.ic3.gov/media/2009/090331.aspx. on 29/03/2019

International Police (INTERPOL) (2011). Access from: www.interpol.org. on 25/03/2020

International Telecommunications Union. (2008). Africa, ICT Indicators 2007, ITU World Telecommunication/ICT Indicators Database, Geneva.

Johnson, G. M. (2010). Young children's Internet use at home and school: Patterns and profiles. *Journal of Early Childhood Research*, *8*(3), 282-293.

Jones, C. R. (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) pp. 129-137.* Retrieved from: online@http://www.interesjournals.org/JPGD on 10/10/2019

Kamal, M. M., Chowdhury, I. A., Haque, N., Chowdhury, M. I., & Islam, M. N. (2012). Nature of cybercrime and its impacts on young people: A case from Bangladesh. *Asian Social Science*, *8*(15), 171.

Key, J. P. (1997). Questionnaire and Interview as Data—Gathering Tools. *Oklahoma State University: Stillwater, OK, USA*

Kwablah, E. (2009). Cybercrime: Giving a bad name to Ghana. *Business and Financial Times*.

Magele, T. (2005, February 16/17). *E-security in South Africa*, White Paper prepared for the Forge Ahead e-Security event. Retrieved from: www.forgeahead.co.za/. on 25/02/2019.

Martis, P. L. (2018). Cyber Crime Awareness among Youth in Udupi District. *Journal of Forensic Science and criminal investigation Volume - 8 Issue 5*.

Meke, E. S. N. (2012). Urbanization and Cyber Crime in Nigeria: Causes and Consequences. *European Journal of Computer Science and Information Technology*, *3*(9), 1-11.

Merton, R. K. (1968). *Social Theory and Social Structure* (1968 enlarged Ed.). New York, NY, US: Free Press.

Merwe, C. V. (2015). *The Nature and Extent of Cyberbullying of Senior High School Students at Abbotts College (Century Gate Campus) (Bachelor's Degree Thesis).* University of South Africa.

Miniwatts Marketing Group (2017). *Internet Usage Statistics for Africa* [online]. Access from: http://www.internetworldstats.com/stats1.htm on 27/05/2020

Morgan, S., & Park, M. (2019). Cybersecurity Ventures Official Annual Cybercrime Report (2018).

Nilson Report (2019). Card Fraud Losses Reach $27.85 Billion worldwide. Retrieved from: https://nilsonreport.com/mention/407/1link/# on 29/09/2019

Ninalowo, A. (2016). *Nexus of state and legitimation crisis*. Lagos: Prime Publications.

Obiri Yeboah, N. L. (2015). *An Investigation of Youth in Cybercrime in the Ayawaso East Constituency of Greater Accra* (Doctoral dissertation, University of Ghana).

Odo, C. R., & Odo, A. I. (2017). The extent of involvement in cybercrime activities among students' in tertiary institutions in Enugu State of Nigeria. *Global Journal of Computer Science and Technology*.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98-114.

Olayemi, J. (2014). "Combating the Menace of Cybercrime". *International Journal of Computer Science and Mobile Computing, Vol.3, Issues 6, pp.980-991.*

Oluwadare, C. T., Oluwasanmi, L. A., & Igbekoyi, K. E. (2018). Prevalence and Forms of Cybercrime Perpetrated by Students in Public Tertiary Institutions in Ekiti State. *International Journal of Arts, Languages and Business Studies*, *2*(1).

Orji, U. J. (2018) *International Telecommunications Law and Policy*. United Kingdom: Cambridge Scholars Publishing.

Orji, U. J. (2018). The African union convention on cybersecurity: a regional response towards cyber stability. *Masaryk UJL & Tech.*, *12*, 91.

Parker, D. B. (1980). Computer abuse research update. *Computer/LJ*, *2*, 329. Retrieved from:https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmjcila2&div=24&id=&p age=&t=1557327033. on 18/04/2019.

Punch, K., F. (2005). *Introduction to social research: Qoalitative and quantitative approaches*, 2th ed. London,SAGE publication Ltd.

Reasentse, T. (2015). Examining Media Portrayals of and Approaches to Cybercrimes in Botswana. Retrieved from: https://www.academia.edu/12944302/ on 10/10/2019

Regoli, M., & Hewitt, D. (1997).*Delinquency in Society (3rded.).* New York: McGraw-Hill Companies, Inc.

Rose, S., Aburto, M., Hagemann, J., & Shahnazarian, D. (2009). Informed consent in human subjects research. *University of South California.[Online]*. Retrieved from: https://oprs.usc. edu/files/2017/04/Informed-Consent-Booklet-4.4, 13 on 29/09/2019.

Salifu, A. (2008). Impact of Internet crime on development. *Journal of Financial Crime, 15*(4), 432–444.

Salkind, N. J. (Ed.). (2010). *Encyclopedia of research design* (Vol. 1). Sage.

Sarantakos, S. (2013). *Social research*, 4th ed. New York, Palgrave Macmillan.

Schjolberg, S., & Ghernaouti-Helie, S. (2011). A global treaty on cybersecurity and cybercrime. *Cybercrime Law, 97.*

Schmalleger, F., & Pittaro, M. (2009). *Crimes of the Internet.* Saddle River, NJ: Pearson Prentice Hall.

Security Engineering Research Team (SERT, 2016) Threat Report. *SERT Quarterly Threat Report Q2 2016*, NTTSecurity. Retrieved from https://technical.nttsecurity.com/post/102dwj0/q2-16-quarterly-threat-intelligence-report on 13/03/2019.

Serianu, United State International University-Africa (2016). Ghana Cyber Security Report 2016. Retrieved from: https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf on 25/08/2019**.**

Shehu, Y. A. (2014). Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. *Online Journal of Social Sciences Research, 3 (7),* pp 169-180.

Singh, S. & Bala, J. (2014). Utilization pattern of internet among secondary school students. *Asia Pacific Journal of Multidisciplinary Research*, 2 (6). Retrieved from: www.apjmr.com on 13/12/2019

Snail, S. (2009). Cyber Crime in South Africa–Hacking, cracking, and other unlawful online activities. *Journal of Information, Law and Technology, 1, 2009.*

Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, *58*(1), 22-23.

Sutherland, E., & Cressey, D. (1978). *Principles of Criminology (10th ed.)*. Philadelphia: Lippincott

Sutherland, E. H. (1939). *Principle of Criminology*. Philadelphia: Lippincott.

Tapestry networks (2015). *Cyber security in financial institution.* Retrieved from htt//:www.tapestrynetwrks.com/issue./financial on 13/03/2019.

The Association of Chief Police Officers (ACPO, 2013). Benchmarking Police Integrity Programs Transparency International UK

The European Union Cybercrime Law (2013). Access from: https://www.cybercrimelaw.net/EU.html 25/03/2020

Types of Cybercrime (2018). Panda Security. Retrieved from: https://www.pandasecurity.com/mediacenter/panda.../types-of-cybercrime/ on 07/06/2019.

Uddin, M., and i Hasan, M. (N. D.). Impact of internet use on young students of Bangladesh. Retrieved from: https://www.google.com/url?s2FImpact_of_internet_use_on_young_students_sg=AOv on 27/09/2019

United Nations Economic Commission for Africa (UNECA) Press Release (N.D.). *Draft African Union Convention on Cybersecurity Comes to its Final Stage*. Access from: http://www1.uneca.org/TabId/3018/Default.aspx?ArticleId=1931 on 25/03/2020.

U. S. Department of Justice, Background on the G8 (2004). Access from: https://www.justice.gov/archives/ag/g8-background on 25/03/2020

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, *5*(1), 736.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

APPENDICE

APPENDIX I: QUESTIONNAIRE

I am a graduate student of the University for Development Studies, undertaking a study on the topic: **Assessment of the Perceptions on the Effects of Cybercrime on Senior High Students in Tamale Metropolis: A Case Study of Vitting Senior High School.** This study is part of the requirements leading to the award of a Master of Philosophy Degree in Development Education. *Your participation in the study is completely voluntary. You are also assured that the information you provide will be treated as confidential and used for academic purposes only.*

Thanks a lot for your participation. In case you have any questions, please let us know. Please also ask when you have a problem understanding a question.

Thank you.

INSTRUCTION: Please **tick/mark (√)** in the box and write where necessary.

A. **Socio-demographic Characteristics**

1. Gender of respondent

a. Male ( )
b. Female ( )

2. Age of respondent

a. 13-15years ( )
b. 16-18 years ( )
c. 19-21 years ( )
d. 22-24 years ( )
e. 25 and above ( )

3. Whom do you live with at home?

a. Father ( )
b. Mother ( )
c. Both Parents ( )
d. Guardian ( )

4. Marital Status of parents/guardian?

a. Single ( )
b. Married ( )
c. Divorced ( )
d. Separated ( )

5. Educational level of parents/guardian

a. None
b. Primary
c. JHS
d. SHS
e. Tertiary

6. Course of respondent

a. Agriculture ( )
b. Home Economics ( )
c. Technical ( )
d. Visual Art ( )
e. General Art ( )

7. Level/form of respondent

a. SHS 1 ( )
b. SHS 2 ( )
c. SHS 3 ( )

8. Residential status

a. Day ( )
b. Boarder ( )
c. Hostel ( )

B. Prevalence of cybercrime among students in Vitting Senior High School

Rank on a Likert scale of **1-5** to what extent of cybercrime/Sakawa among students.

Strongly Agree (SA) = **5** points, Agree (A) = **4** points, Neutral (N) = **3** point, Disagree (D) = **2** points and Strongly Disagree (SD) = **1** point.

9. How prevalent is cybercrime/sakawa among students of Vitting SHS?

a. Very common ( )
b. Common ( )
c. Not common ( )
d. Non-existence ( )

10. Extent of cybercrime/Sakawa among students	**5**	**4**	**3**	**2**	**1**
Students sent e-mails to impersonate credible institutions to steal personal or financial information via a contaminated link.					
Students use the credit card of other people illegally to buy goods and services online.					
Students deceive and manipulate investors resulting in stealing of capital through fake documentation					
Students steal trade secret, suppliers' agreement, personal records, research documents, to order for goods and services online.					
Students do send email to internet users portraying themselves as legitimate business owners to scam users into giving out private information that will be used for identity theft					
Students use special hacking software to infiltrate financial institutions records on the internet.					
Students buy goods and services online without paying					
Students use international money transfer agencies (i.e. western union, money gram) to carry out a scheme to defraud people.					
Students persuade people to invest in a non-existent business on the internet, eg gold					
Students use dating sites to deceive and manipulate people resulting in stealing of capital.					

C. Knowledge level of students on cybercrime

11. Do you browse the internet?

a. Yes ( )

b. No ( )

12. Do you have an e-mail/Facebook account?

a. Yes ( )

b. No ( )

13. What information do you normally browse for? Choose any option that applies

e. For studies ( )

f. Sending/checking e-mails ( )

g. Searching for software ( )

h. Facebooking ( )

i. Others, please specify ( )

14. Have you heard of cybercrime/sakawa?

a. Yes ( )

b. No ( )

15. How do you get to know about cybercrime or Sakawa? Choose any option that applies

a. From friends

b. From the internet

c. From radio

d. From school mates

e. Others

16. Do you know anybody who is engaged in cybercrime/sakawa?

a. Yes ( )

b. No ( )

17. Have you ever engaged in cybercrime or sakawa?

c. Yes ( )

d. No ( )

18. Do you think that peer influence affects your knowledge on cybercrime/sakawa?

a. Yes ( )

b. No ( )

19. Describe cybercrime/sakawa in your opinion

……

……

……………………………………………………………………………………………..

Rank on a Likert scale of **1-3**on the knowledge level of students in cybercrime/Sakawa.

Good (G) = **3** points, Fair (F) = **2** points, Poor (P) = **1** point

20. Identify a type Cybercrime/Sakawa that is commonly practiced by students.	**3**	**2**	**1**
Upload female pictures without their consent to deceive people online			
Hack into people's personal and sensitive information in internet			
Asking people to invest in a non-existent business on-line (Business Fraud)			
Stealing a trade secret, supplier agreement, personal records, and research documents for financial gain (Industrial espionage)			
The use of another person's name and social security number to obtain goods and services (identity theft)			
The act of sending an e mail to internet users falsely claiming to be an established legitimate enterprise in an attempt to scam the users in to surrendering private information that will be used for identity theft (phishing)			
Practice of deceiving and manipulating investors resulting in theft of capital (investment fraud)			
Creation and distribution of computer viruses			
Cybercrime with direct contact through phone call (social engineering)			
Hacking of organizational account.			

D. Effects of cybercrime/sakawa on academic performance of students

Rank on a Likert scale of **1-5**on the effects of cybercrime/sakawa on academic performance of students. Strongly Agree (SA) = **5** points, Agree (A) = **4** points, Neutral (N) = **3** point, Disagree (D) = **2** points and Strongly Disagree (SD) = **1** point.

21. Does cybercrime/sakawa have any effects on student's performance?

a. Yes ( )
b. No ( )
c. No idea ( )

22. What is the nature of effect does cybercrime/sakawa have on student performance?

a. Positive ( )
b. Negative ( )
c. No idea ( )

23. Perceived effects of cybercrime on academic performance of students	**5**	**4**	**3**	**2**	**1**
Poor academic performance					
Poor school attendance (Absenteeism)/class can lead to low academic performance					
Decrease ability to concentrate					
School drop out					
Getting arrested by police					
Going to jail					
Stigmatization					
Parental disownment					
Defamation of image of Schools					
Students who are engage in cybercrime spent more time on the internet browsing than reading/revising their books					
Sexual promiscuity					
Socially and mental harassment					
Students earn enough income to cater for their needs					

E. Factors that influence students to engage in cybercrime/Sakawa

Rank on a Likert scale of **1-5**on factors which influence students to engage in cybercrime/sakawa. Strongly Agree (SA) = **5** points, Agree (A) = **4** points, Neutral (N) = **3** point, Disagree (D) = **2** points and Strongly Disagree (SD) = **1** point.

24. Factors that influence students into cybercrime (Sakawa)	**5**	**4**	**3**	**2**	**1**
Pressure from, Friends, Relatives, School mates, Colleagues in my area					
Get-Rich-Quick syndrome					
Poverty					
Fame (Societal Recognition)					
Knowledge of internet literacy					
Students see cyber fraud/sakawa as creative thinking					
Students see cyber fraud/sakawa as a place to deploy their knowledge					
Poor parenting					
Instant wealth is equated with smartness					
Attitude of leaders towards wealth					
Cybercrime is viewed as social exposure					
Students see cybercrime/sakawa as a means to payback the white man for taking their forefathers as slaves and stealing resource from Africa.					
Because it is easy to practice and difficult to be identified					
Cybercrime victims mostly go unpunished					

Any other comments? ....

Thank you very much for your time and participation.

APPENDIX II: INTERVIEW GUIDE

Participants (Interviewees):

Assistant Headmaster in charge of academic

&

Senior house masters

I am a graduate student of the University for Development Studies, undertaking a study on the topic **Assessment of the Perceptions on the Effects of Cybercrime on Senior High Students in Tamale Metropolis: A Case Study of Vitting Senior High School.** This study is part of the requirements leading to the award of a Master of Philosophy Degree in Development Studies. You are assured that the information you provide will be treated as confidential and used for academic purposes only.

Thank you.

1. In your opinion what do you think cybercrime is?

   Probes: Definition

2. What is the situation like on campus regarding cybercrime?

   Probes: Is it common practice amongst students

   Do you receive complains about students engagement in cybercrime/sakawa practice?

   Do students in this school engage in cybercrime/sakawa?

   To what extent do students engage in the practice of cybercrime/sakawa

   How different is it from other forms of crime?

3. What do you think are the main causes of these practices among the students?

4. What do you think are the effect of cyber-crime practices among SHS students in Ghana?
5. What do you think can be done to minimize/prevent cybercrime among SHS students in Ghana?