UNIVERSITY OF EDUCATION, WINNEBA

CYBER FRAUD AMONG THE YOUTH IN GHANA: THE CASE OF SOME STUDENTS IN A PRIVATE UNIVERSITY

AMIDU AYAM HAMZAH
202122838

A thesis in the Department of Strategic Communication, School of Communication and Media Studies, submitted to the School of Graduate Studies in partial fulfilment of the requirements for award of the degree of
Master of Arts
(Strategic Communication)
In the University of Education, Winneba

NOVEMBER, 2022

DECLARATION

Student's Declaration

I, Amidu Ayam Hamzah declare that this thesis, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my original work, and it has not been submitted**,** either in part or whole, for another degree elsewhere.

Signature: ....

Date: ....

Supervisor's Declaration

I hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of Thesis as laid down by the University of Education, Winneba.

Name of Supervisor: Dr. Albert Agbesi Wornyo

Signature: ....

Date: ....

ACKNOWLEDGEMENTS

First and foremost, I thank Almighty Allah for taking Good care of me during my time at this excellent university. I would want to offer my heartfelt gratitude to everyone who assisted me in the preparation of my thesis in various ways. I owe a special thanks to Dr. Albert Agbesi Wornyo, my project supervisor. Without his guidance, this project would not have been successful.

I would also like to express my gratitude to Prof. Andy Ofori-Birikorang, PhD, Dr. Mavis Amo Mensah, Dr. Akwasi Bosompem Boateng, Mr. Kwesi Aggrey, Mr. Rainbow Sackey Mr. Bismark Odum-Sackey, and Ms. Cecilia Agyapong for their academic and social support throughout my stay in Graduate school. I appreciate your valuable inputs.

I would want to express my heartfelt gratitude to Angela Asiedua Siaw, Vivian Sedzro, Ernest Kofi Offin, Manasseh Bagmarigu, Sampson Shadrach Daniels, and Emmanuel Darko for their unwavering support. You're the greatest!

To the 2021/2022 CoMSSA group, especially my closest Andrews, Jonathan, and Dominic, who have shared exciting ideas with me, I say , Let's keep chasing our dreams.

I would like to express my gratitude to my senior sister Nabia and my immediate elder brother Majid, both of whom have been financially supportive of me. Finally, I would want to express my heartfelt gratitude to my wonderful mother, Madam Ayishetu, who has cared for me since I was a child till now. May Almighty Allah provide you long life and strength so that you can enjoy the fruits of your labor.

DEDICATION

Special Dedication to my parents and siblings who made my dream a reality.

TABLE OF CONTENTS

ABSTRACT

This study investigates cyber fraud among the youth in Ghana. The objectives of the study was to investigate the scope of cyber fraud, explore the factors that motivate the youth in engaging in cyber fraud and also examine their perspectives about how to curb cyber fraud. Using qualitative research approach and snowball sampling technique, the study purposively selected ten students from Wisconsin University and the Academic City University. The theories that underpin this study are the space transition theory and the theory of routine activity. Data were collected through unstructured interviews. The data were analyzed thematically. It was revealed that cyber fraud serves as a remedy for unemployment for those who engage in it. For some of the country's youth who were unemployed. The study indicated that, most university students who engage in Cyber fraud are introduced to it by either their relatives or colleagues. It was found that the desire for financial gain was the driving force behind their participation in cyber fraud. The study recommends that relevant security authorities such as the ministry of communications carry out intensive public education on how to identify Cyber fraud. The government also needs to intensify its attempts to create jobs for more of the youth that are unemployed to get themselves means of earning income.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Cyber fraud began prior to actually Microsoft Windows, the Internet, or the personal computer (PC) (Thomas, 2008). The first recorded instance of cyber fraud occurred in 1964, when a student at the Massachusetts Institute of Technology (MIT) used an MIT computer to mimic the tones required to access long distance phone service (Thomas, 2008). Crimes committed over the Internet have become more sophisticated since 1964, with the perpetrator taking greater risks to commit the crime. The Bulletin Board System (BBS) was established in 1978. (Thomas, 2008). A bulletin board system (BBS) is a computer or software program that allows users to share and exchange messages and other files via a network. Simple messages were exchanged between users through the use of the BBS. Before the World Wide Web, the BBS was the most common type of online community in the 1980s and early 1990s. Ward Christensen and Randy Suess established the first BBS, the Computerized Bulletin Board System (CBBS), in 1978. Using a modem and a telephone, the system allowed computers all over the world to communicate with one another. As the BBS grew in popularity, so did the number of computer experts and hackers (Thomas, 2008).

When the third version of Microsoft windows (Win3.X) was the primary operating system of personal computers in the early 1990s, the user had to configure the settings in a text editor, using computer jargon (Thomas, 2008). To gain access to the Internet, some hacking and programming were required (Thomas, 2008), resulting in the true beginnings of cyber fraud.

Unauthorized access, denial of service attacks (DoS), cyberterrorism, cyberstalking, identity theft, and phishing emerged soon after. The number of reported cyber fraud has increased. In 2007, more than 90,000 of the 206,884 Internet crimes reported in the United States were referred to law enforcement agencies (IC3, 2008). In addition, financial losses increased by $40 million in 2007 compared to the previous year (IC3, 2008).

Information and communication technologies (ICT) penetration and adoption are increasing across Africa, compared to a few decades ago (ITU, 2008). While most parts of Sub-Saharan Africa still rely on public internet access points like cybercafés for basic internet and other online services, country's like Nigeria, Cameroon, and Ghana now have satellite connections and fiber optic cables to provide mobile internet access. This rise in ICT penetration, especially along the West African coast, has resulted in an increase in ICT-based businesses and services such as electronic government, electronic commerce, teledemocracy, telemedicine, and electronic banking.

Unfortunately, this level of globalisation, which is aided by ICTs, has also increased the prospect of new criminal activity seeking to profit from it. The internet has become a two-edged sword, offering opportunities for individuals and businesses but also increasing the possibility of information security breaches (Magele, 2005).
A common understanding of the term cyber fraud is required before a person can fully comprehend the magnitude of cyber fraud statistics. According to (Babu & Parishat, p. 1), cyber fraud is "a criminal activity committed on the Internet." It is a broad term that encompasses everything from electronic cracking (illegal access to computer

information or systems) to denial-of-service attacks that cause online retailers to lose money" (Babu & Parishat, p. 1).

Today's law enforcement agencies and state legislatures face two challenges, Hardesty and Ball (NWCCC, 1996). First, there is a need for a consistent, clear, and concise definition of cyber fraud. Second, there is a need for data collection and sharing among agencies and states. Hardesty and Ball (NWCCC, 1996) went on to argue that defining white-collar crime, particularly cyber fraud, would be a significant step towards understanding the crime.

Hardesty and Ball (NW3C, 1996) believed that three factors would lead to cyber fraud deterrence and retribution. These factors include a clear definition of cyber fraud, comprehension of the crime, and proper investigation. If the methods of investigation are included in the definition of cyber fraud, common procedures can be established. The adoption of uniform procedures increases the likelihood of apprehending and convicting the criminal. From the viewpoint of ICT for development, it is fair to say that cyber fraud poses some risks and has the potential to curtail the developmental benefits that can be reaped from well-managed ICT adoption, dissemination, and use in Sub-Saharan Africa. Cyber fraud has the ability to deepen the digital divide, inflict damage on the information infrastructure, and weaken consumer confidence in online transactions (Salifu, 2008; Longe et al., 2009; Oumarou, 2007).

However, there is a lack of research on the nature of these fraudulent cyber operations in different countries, as well as the steps taken to combat them. For instance, Ghana, the study's focus country, was ranked among the top ten countries in the world for the source of fraudulent cyber activities, with Nigeria coming in third in the 2008 Internet

Crime Complaint Center Report (IC3, 2008). Ghana's government has made significant efforts to turn the country into a "knowledge-based economy," The Ghana ICT for Accelerated Development (ICT4AD) Policy (2003).p.6 making it an ICT-driven economy.

After the economic reforms of the telecommunications industry in the 1990s, Internet use in Ghana has increased significantly. In 2008, the country had 43 Internet users per 1,000 residents, compared to one in 1999. International Telecommunication Union (ITU, 2009). Between 1999 and 2005, the number of Personal Computer owners doubled to 52 per 1,000 people, International Telecommunication Union (ITU, 2007). With these advances come the unforeseen consequences and negative effects of ICT, especially cyber fraud. The aim of this project is to investigate the factors influencing student into cyber fraud / sakawa as well as the steps in place to combat them and facilitate the identification and tracking of suspects in cyber-fraud cases.

1.2. Statement of the Problem

Over the previous few decades, technological advancements have aided in a transformation in how people use computers. The introduction of the World Wide Web/Internet aided in the transformation of communications and transactions (Holt and Bossler, 2014). Computers and the internet have become a global phenomenon in recent years.

Technology today connects people all over the world in ways that were never possible before. Citizens from distant countries can communicate easily thanks to the connectivity of many computers, known as ‘cyberspace.’ Regrettably, as online has grown and changed, so have cybercrime in all of its manifestations. New technology creates new potential for new crimes, and the number of cybercrimes reported to authorities has risen dramatically (Wang, 2007; Nuth, 2008, Walden, 2004).

The fast growth of e-commerce in the United States has surely enhanced the threat of cybercrime (Oates, 2001). Increased information and communication technology, lower transactional costs compared to traditional (brick and mortar) establishments, and increased rivalry and productivity by firms are all factors contributing to this explosion (Ramcharran, 2013).

Due to the expansion of e-commerce, which allows rivalry between traditional (brick and mortar) retail sales and e-commerce (Internet) sales, the Internet has also affected the economic culture of U.S. customers (Ramcharran, 2013). According to the findings, Internet costs are 9-16 percent lower than those in traditional stores (Ramcharran, 2013). Consumers are increasingly turning to this new technology to shop for bargains online (Holt and Bossler, 2014).

Cyber security is "one of the most significant economic and national security concerns we face as a nation," according to the US government (Kaplan, Sharma, and Weinberg, 2011, p.7). Cybercriminals or disgruntled workers may pose a threat by stealing or misusing business information, intellectual property, or online fraud, in which victims are exposed and asked to pay a ransom for the information taken (Kaplan et al., 2011).

The shift to online or digital commerce, which offers a target-rich environment for cybercriminals eager for a big payday, has resulted in an upsurge in attacks (Kaplan et al., 2011). The Council of Europe (CoE), a 47-country European body, established a

Committee of Experts on Crime in Cyberspace in 1997 to identify and define new crimes, jurisdictional rights, and criminal liabilities related to the Internet.

As observer states, Canada, Japan, South Africa, and the United States were invited to participate in the debates. The goal was to develop a set of global standard laws on cybercrime as well as a common criminal policy to combat cybercrime. The country representatives aimed to make it easier for law enforcement to collaborate in the collection of evidence for computer crimes investigations (Furnell, 2002).

Analysts have stated that 10–15 percent Internet penetration is the threshold level for the development of substantial hacking operations, based on the trajectory of cybercrime across countries (Kshetri, 2013). Many African economies have already attained this level of internet penetration. "Cybercrime is going towards emerging economies," said Bulent Teksoz of Symantec Middle East. The cyber crooks assume here is where the "low-hanging fruit" is. Many African economies have become key sources as well as victims of cyber-threats, which is unsurprising.

According to the Global Internet Report (2015), Ghana ranks second among West African countries with the highest cyber fraud, (Sakawa) and seventh among the top ten countries with the fastest-growing cyber fraud records (Abugri, 2015). According to Abia et al. (2010), 15% of Ghanaian students are cyber fraudsters or engage in (sakawa), 95% of students make friends with fraudsters, and 65% of fraudsters or youth who engage in (sakawa) lose concentration on their education and ultimately drop out.

Ghana's government has acknowledged that cyber fraud is a threat to the nation and is taking steps to fight it (Warner, 2011). About 15% of today's school-aged youth in

Ghana are practicing cyber fraud (sakawa) Abia et al. (2010), and even some of those still pursuing their education at the university level indulge in the act while schooling. According to Igba Daniel et al. (2020), there are few options for dealing with the problem of cyber fraud, and therefore further research in this area is required. This study seeks to investigate cyber fraud among the youth in Ghana specifically some students in a private university.

1.3 Purpose of the Study

The main purpose of the study is to examine the scope of cyber fraud among the youth in Ghana using some students in a private university as a case study through the perceptions and lived experiences of practitioners.

1.4 Research Objectives

1. Investigate the scope of cyber fraud among the youth in Ghana.
2. Explore the factors that motivate the youth to engage in cyber fraud.
3. Examine the perspectives of the youth about how to curb cyber fraud among the youth in Ghana.

1.5 Research Questions

The following questions formed the basis of this research.

1. What is the scope of cyber fraud among perpetrators?
2. What factors motivate the youth to engage in cyber fraud?
3. What are the perspective of the youth about curbing cyber fraud among the youth in Ghana?

1.6 Significance of the Study

Individuals, societies, the nation, and the world as a whole will benefit from this research. The study's findings exposed the scope of cyber fraud and the factors that motivates the youth to engage in cyber fraud. The findings of the research will be useful for government agents and other stakeholders such as the police and criminal justice departments.

It will also be valuable to policymakers and experts who are developing cyber fraud policies in the country. Readers will be made more aware of cyber fraud and other relevant matters as a result of the study. It will not only broaden readers' knowledge, but it will also act as a resource for experts and students of all fields who want to learn more about cyber fraud and its repercussions.

1.7 Organization of the Study

The research is divided into five chapters. The first chapter contains the study's introduction, which includes the study's background, which examines cyber fraud around the world before narrowing it down to the study area. The problem statement also addressed the gap in the study of cyber fraud. The chapter further discusses the study questions and objectives for which the study aims at achieving. It also outlined significance of the study which indicated the importance of the study to society.

Chapter two looks at a review of the available literature relevant to the work, it encapsulates the general concepts of the study and theory used to anchor the study.

Chapter three outlined the research methodology adopted in conducting the study. This includes the Introduction, Research Approach, Research Design, Sampling and Sample Technique, Sources of Data, Data Processing and Analysis, Field Entry Processes, Ethical Considerations, and Issues from Field. Additionally, validity and reliability of the data, limitations and delimitations were all captured under chapter three. Chapter four comprises discussions on the study's findings. The issues covered involved the scope of cyber fraud to enable readers to get the basic understanding of cyber fraud. The concluding chapter, chapter five deals with the summary of major findings from the study, conclusions drawn from the findings and recommendations made to ameliorate the situation.

1.8 Chapter Summary

This chapter introduced the study with a background of the history of cyber fraud. It discussed how information and communication technologies (ICTs) are now more widely used and adopted in Africa than they were a few decades ago. It also discussed how ICT-based businesses and services have increased ICT penetration throughout West Africa. The chapter also highlighted the extent of globalization made possible by ICTs as a potential source of new criminal activities. Minimal studies have been conducted on the scope of cyber fraud especially in the Ghanaian context.

CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.0 Introduction

This chapter focuses on reviewing extant literature on new media and cyber fraud. The chapter also discusses the theoretical framework that guided the study. The study used two main theory which is Routine activity and the space transition theory. Relevance of the theory to the study was also discussed.The chapter discussed The Concept of Cyber Fraud, Practices of Cyber Fraud and The Effects of Cyber Fraud to Victims and the development of the Country. Legal processes for dealing with cyber fraud was also dealt with. Researchers' studies were also examined as empirical proof for this work. It concludes with a summary of the study's conceptual frameworks. Cyber fraud and how it is perpetrated are explained in the conceptual frameworks.

2.1 New Media and Cyber Fraud

The 21st century is marked with the massive proliferation of technological devices and tools which have made it possible for virtual communities and interaction to be enhanced in the whole wide world. One technological that has been the backbone for the new media technologies is web 2.0. Web 2.0 which has made it possible for internet platforms to create user interactive applications that allows users to be both producers and consumers of online content.

Jones, Malczyk and Beneke (2010) opined that the entire premise of web 2.0 is based on the ability to network with peers and likeminded communities using technology. This phenomenon is broadly categorized as social media. Social media is an umbrella term for all web 2.0 enhanced technologies, application and webs that allow users to communicate in real time or at different times via an online space.

Social media platforms come in different forms such as general sites that are accessible to all and sundry like WhatsApp, Facebook, and others that are securely limited to serious and intricate business networks such as LinkedIn. Other social media platforms are focused on well-defined community pages while others are difficult to be categorized because of their unique tools, features and devices. But as asserted by Jones, Malczyk and Beneke (2010), social communities facilitated by social media platforms have sprung up around hobbies, locations, causes, beliefs, creative works and even brands. They have incredible power to steer opinions and spread messages, making them both extremely valuable and very risky to use.

New media is basket of fresh and rotten fruits as well as opportunities and threats that need to be regulated to produce possible outcome for society (Manyika, 2007). The potential benefits of new media in changing the status quo of human life in all areas is proportionally sandwiched by the new opportunities for criminals to exploit and cost men lots of harm (Adam & Berenblum, 2019).

No wonder Heidegger's (1977) commented that 'the essence of technology and its uses is much more ambiguous' (Heidergger & Lovitt, 1977). This means that despite the embedded significance of new media in the political, social and economic life of society, there are equally insulated implications that threaten the survival of benefits society derive from new media except those threats are minimized if not mitigated.

As Adam and Berenblum (2019) posited that the Internet, computers, cell phones, and other forms of technology have revolutionized every aspect of human life over the last several decades, including how we communicate, bank, shop, obtain the news, and entertain ourselves. They were also quick to add that these technological advancements have also created myriad opportunities for offenders to commit various forms of crime. Cyber fraud is the term given to crime which evolved from new media use or technology.

Cyber fraud is one of the major dark sides of new media that has attracted the attention of research in recent time (Sarre, Lau & Chang, 2018). Online crimes are often referred to as cyber fraud and occur because 'the perpetrator uses special knowledge of cyberspace' (Furnell, 2002, 21). Even though the concept cyber fraud is multifaceted, scholars have proposed some conceptual definitions.

McGuire and Dowling (2013) defined cyber fraud as a large umbrella term that encompasses computer-assisted crime in which computers and technology are used in a supporting role to commit the crime or computer-focused crimes that are a direct result of computer technology and would not exist without it, such as unauthorized computer system trespassing. Cyber fraud differ from traditional crime because cyber fraud is usually perpetrated through the assistance or urgency of new media technologies.

There are varied forms of cyber fraud such as vishing, phishing, virus attack, cyber defamation among others. These diverse forms of cyber fraud affect various aspect of the society negatively. For instance, child pornography has the potential to deteriorate the moral values that are established in society. Likewise, phishing and vishing have the potential to distract online marketing and financial services and therefore affecting economic activities. In essence, the myriad of opportunities provided by new media to extend daily crime to online space is gradually affecting lives and properties across the globe and there is the need for governments to collaborate to find solutions to the canker called cyber fraud.

The task looks huge because of the fast pace at which cyber fraud is evolving, there is possibility of academia liaison with policy makers to provide empirical evidence that can bark policy making for combating cyber fraud (Sarre, Lau & Chang, 2018).

While this call is vital and key in the continuity of national security and individual privacy security in the cyberspace, there is little available studies on how policy making could act as mitigating factor among other factors in combating cyber fraud. This paper presents the available literature in this area in order to draw valuable conclusions and recommendations that can derive future studies. The researcher synthetizes seven peer reviewed journal articles which are related to the topic and synchronize them within the lens of my understanding in the sessions in this course on Media and Technology.

Sarre, Lau and Chang (2018) remarked that there is no precise and clear definition of cyber fraud in academic parlance based on the difficulty in selecting a concept that capture cyber fraud. Terminologies such as 'electronic crime,' 'computer crime,' 'computer-related crime,' 'hi-tech crime,' 'technology enabled crime,' 'e-crime,' or 'cyberspace crime' (Chang, 2012) have been used to describe one and the same thing, thus a crime committed on the cyberspace.

Despite the diversity in terminologies, cyber fraud tend to be mostly used by scholars to describe the phenomenon of online or internet or new media-based crime.

Therefore, Gandhi (2012) defined cyber fraud as a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks.

Gandhi (2012) extended to definition of cyber fraud to include the context of national security whereby activism, traditional espionage, or information warfare and related activities are likely to be dominant. Perhaps, the nature of cyber fraud informed Saini, Rao and Panda (2012) description of cyber fraud as global problem. It is a global problem because it can cut across borders of nation state and perpetrators are not easily identifiable.

2.2 Cyber Fraud Prevalence

There are evidences of the rate at which cyber fraud is occurring in different parts of the world. According to Consumer Reports State of the Net (2007), it shows that more than $7 billion cost of cyber fraud on U.S consumers was estimated. The Internet Crime Compliant Centre (2012) reported that victims had losses over $500,000. In 2012, the Internet Crime Complaint Centre (IC3) received 289,874 consumer complaints, with losses of $525,441,110 (Ndubueze, 2013).

In Nigeria, Ndubueze (2013) shows 8.3% increase in losses from the previous year and the most affected victim complaint country was the United States with 91.2%. The most frequently reported cyber fraud complaints were auto fraud, military impersonation, e-mail scam, romance scam, intimidation/exploitation scam and among others as stressed by Ndubueze, (2013).

According to Bengal et al, (2012), the prevalence appraisal of a survey was used to estimate how many of Nigerian's 48.3 million internet users experienced the loss. This was used to compute the estimated loss for Nigeria. The case of Ghana is not different in that different figures ranging 2 million cases are circulating online on cybercrime cases.

2.3 Forms of Cyber Fraud

All cyber fraud or crimes are not the same. Oluwadare, Oluwasamni, and Igbekoyi (2018) identified a number of cyber fraud. One, e-mail scam and spam is a cyber-fraud where cyber fraudsters' uses these patterns to solicit and present false investment to their unsuspected victims.

The authors argued that locally and internationally, Nigeria's image has been seriously dented by the above schemes of cyber fraud such that, there is a type of e-mail scam code named the 'Nigerian' E-mail scam. Another cyber fraud is cyber stalking. There is no universally accepted definition of cyber stalking as posited by Martin (2016). It is generally considered as the use of internet, e-mail or other electronic communication devices to harass a person(s) and thereby causing an injury or damages to the victim.

Furthermore, hacking, according to Martins (2016), is a form of cyber fraud which include illegal access, hijacking, bombing, denial of service attack, eavesdropping etc. Some internet users assumed that hacking is harmless, fun and even quite clever, but it can be a serious invasion of privacy and a significant threat to e-commerce.

Another cyber fraud is ATM Fraud. This type of fraud is perpetrated through the ATM machines and e-transaction system. In some cases, the criminals set up their own ATM machines in which the criminal steal the PIN of the users or their cards and use it to withdraw all the money in the victim's account (Martins, 2016).

Again, Oluwadare et al. (2018) identified illegal e-lotteries. It is the effort to get rich quickly by most Nigerians especially the youth is often exploited by cyber fraudsters who send all kinds of tempting messages of an existing lottery bonanza where participants can be deceive with all sorts of items and money ranging from cars, electronics, laptops etc. this form of cyber fraud is rampant in Nigeria (Martins, 2016).

Finally, advance fee fraud: this is where fraudsters obtain money fraudulently from some foreign nationals, mostly Americans, on the promise of getting married to them or an oil contract. These fraudsters extort money from their victims, promising to be in love with them and agree to marry them and in the process demand for money in which they will use to travel and meet them abroad.

2.4 Grabosky's Classification of Cyber Fraud

Grabosky (2007) classified three general forms base on the role of computer in the crime. First form uses computer as the instrument of crime; while the second form uses computer as incidental to the offense, and last form is where computer is the target of crime.

In another classification, Gordon and Ford (2006) classified cyber fraud into Type I and Type II offenses using a continuous scale. Type I cyber fraud is a crime which is more technical in nature (e.g. hacking) while Type II cyber fraud is a crime that relies more on human contact rather than technology (e.g. online gambling).

Gordon and Ford (2006) acknowledge that, there could be other forms that do not fall in their classification. The last classification that is relevant in our understanding of cyber fraud is the one proposed by McGuire and Dowling (2013).
They categorized cyber fraud into 'cyber-enabled' crime and 'cyber-dependent' crime in which cyber-enabled crimes are traditional crimes facilitated by the use of computers. Cyber-enabled crimes include fraudulent financial transactions, identity theft, and the theft of electronic information for commercial gain, drug-trafficking,

aberrant voyeuristic activities, harassment, stalking or other threatening behaviors. Cyber enabled crimes are usually existing in society but are extended using the cyberspace.

On the other hand, cyber-dependent crimes are those crimes that cannot exist without the cyber technology. This category of crime is based on cyber technology. For instance, the May 2015 Cryptowall 3.0 ransomware which caused a lot of damaged to a lot of file that is worth quantified in monetary to some firms about USD325 million. But the fact is, this incident could only be possible through cyber technology because the malware was computer generated (Sarre, Lau & Chang, 2018).

Again, the 'hacktivist' who are unknown online users attacking the services of online marketing firms is causing a lot of damage to reputable organizations. Sarre, Lau and Chang (2018) cited the example of the 2010 anonymous hacktivist attack on Mastercard, Visa and Paypal in retribution for their ceasing to transact donations to the WikiLeaks group as an act that caused Paypal an estimated of amount of USD 5.5 million. From these classifications, it is clear we can understand the multifaceted Scope of cyber fraud and its repercussions if not curbed.

2.5 The Concept of Cyber Fraud

The internet or cyber space has recently served as a "carrier of load" for people, companies, and countries. This is so because the internet has made it easier to communicate, conduct business, and educate people. Despite all of the positive aspects of the internet, considerably more criminals use it to violate national security than for other purposes, such as harassing or intimidating victims, downloading pornographic or unlawful content, or downloading stolen music. They are referred to as cyber fraud. Cyber terrorism, child pornography online, cyberbullying, spam, and Cyber fraud are the different types of cybercrimes. Cyber fraud includes online scam.

In West Africa, mainly Nigeria and Ghana, it is frequently referred to as "419" scams or "sakawa," respectively. Many academics have agreed to share their understanding of what Cyber fraud is. However, its actions have sparked some serious new worries about the possibility of undermining nations' socioeconomic advancement (Burell, 2008). The intentional misrepresentation of facts or identity to defraud others is what the Bureau of Justice Statistics defined as Cyber fraud (Rantala, 2004). Cyber fraud is similarly defined by the Department of Justice as fraud that makes advantage of any aspect of the Internet to carry out the planned fraudulent activity (National White Collar Crime Centre, 2008).

The Australian Federal Police defined Cyber fraud broadly as any type of scam scheme that makes use of one or more online services, such as chat rooms, e-mail, message boards, or websites, to present fraudulent solicitations to potential victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other people involved in the scheme.

Another researcher discussed the concept of Cyber fraud by describing it as any fraudulent conduct that uses a computer or other ICT as a target source (Pati ,n.b).These categories might presumably be modified to conceptualize Cyber fraud as the use of online resources to carry out fraudulent acts. Parker (2000) proposed four categories for the functions of the Internet in Cyber fraud. In other words, it acts as a prop for crime, a victim for crime, a tool for crime, or a representation of crime. When utilized as a target for crime, the Internet serves as an object for the crime.

2.6 Practices of Cyber Fraud

Several schools of thought have compiled information on numerous types of Cyber fraud that is being practiced. The top five most common types of Internet fraud were revealed in 2022 by The Identity Theft Research Center (ITRC), in its annual data breach report. The top five types of Internet fraud were also reported by the Internet Crime Complaint Centre in 2010. The most common types of Internet fraud are Confidence/romance fraud (Come and marry me), Advance fee fraud, Online shopping, classified and auction scams, phishing, Banking, credit card and online account scams, according to these two statistics reports.

According to Internet Fraud Watch Statistics, online auction fraud is the most common type of Cyber fraud (Internet Fraud Watch, 2002). In contrast, the Internet Crime Complaint Centre (2010) identified merchandised fraud as the most common type of fraud (IC3, 2010). According to Jegede (2014), credit card Internet fraud is the most widespread worldwide. The forms are explained in some detail.

2.6.1 Phishing

Phishing is another type of online fraud. Phishing is a method where a fraudster poses as another person's email or website. Usually, the fraudster accomplishes this by duplicating the online content of an authentic website onto their newly developed counterfeit website.

In other words, phishing refers to a strategy in which the offenders try to trick the suspected victim into disclosing sensitive information, like passwords, credit card details, and bank account numbers, by using spoof websites (Kunz &Wilson, 2002). Similar to this, Shinder (2000) approved of scammers sending emails to unknowing receivers that falsely claimed to be from a legitimate company. However, the sole purpose of these websites' creation is to attempt to steal users' personal data (IC3, 2008).

Phishing emails may target online auction sites or other online payment services in addition to online banking customers. A typical phishing email instructs online banking users to click a link to update their personal bank account information. If the link is clicked, the victim downloads an application that logs into their bank and sends their login information to a third party (Australian Federal Police). Ghosh claims that "445,004 attacks in 2012 as compared to 258,461 in 2011 and 187,203 in 2010" demonstrate that phishing has been posing a growing threat to people (Ghosh, 2013). The third Microsoft Computing Safer Index Report, which was published in February 2014, estimates that phishing could have an annual global impact of up to $5,000,000.

2.6.2 Identity Fraud and Identity Theft

Growing globalization and a lack of cyber borders have created an atmosphere where identity fraud can flourish both within and outside of national borders (Finklea, 2014). Identity fraud and identity theft are frequently used interchangeably. The two do differ slightly from one another, though. Identity theft is a specific type of identity fraud that involves using another person's personally identifiable information. Identity fraud is a term used to describe a number of crimes involving the use of false identification, though not always a form of identification belonging to another person. However, in this context, identity fraud is preferred to be referred to as identity theft. Therefore, identity theft is the main subject of this study. Identity theft happens when fraudsters steal the victim's personal information in order to profit financially (Finklea, 2014; Newman and McNally, 2005).

The Code of Federal Regulations (CFR) defines identity theft as any fraud done or attempted utilizing another person's identifying information without that person's consent (Finklea, 2014). When a person is not utilizing the Internet, for instance, if crucial documents like your passport or driver's license are lost, this can occur. Other crimes can both facilitate and be assisted by identity theft. In other words, identity theft frequently has connections to other types of illegal behavior (Finklea, 2014).

Identity theft, for instance, may enable other frauds like bank fraud, document fraud, or immigration fraud. It may also be facilitated by other crimes like theft committed during robberies or break-ins. Credit card fraud and other crimes that could be perpetrated using stolen identities were listed as categories of identity theft by Newman and McNally in 2005.

The Federal Trade Commission continues to receive the majority of consumer fraud complaints involving identity theft (FTC). Identity theft complaints raised red flags for the FTC between 2000 and 2008. Despite declining in 2009 and 2010, it climbed once again in 2011 and 2012. Using credit cards Credit card schemes employ credit card numbers to place unauthorized online orders for and purchases of goods and services. These so-called settlers present their victims with more alluring, pricey, but excessive package goods. The settler then makes purchases online using the victim's information without the victim's consent. The objective of this scam is to learn as much as possible about the victim in order to con them in the future.

A victim's personal information, including name, address, work information, and credit card details, are collected in a number of ways. The victim may use any number of means, like filling out a form on a website, making an online purchase and providing credit card, payment, and delivery information, and so on, to supply the information (Kunz and Wilson, 2002 and Jegede, 2014). Some victims' personal information was taken from the databases of reputable companies or organizations and utilized fraudulently by the offender. It is possible that this swindle will be unnoticed by the victim for several months.

2.6.3 General Merchandise Auction

Another type of Cyber fraud involves general products and auctions, in which victims are asked to make payments online but never get any goods (Danquah & Longe, 2011). The bulk (64%) of all online fraud, according to a survey published in May 2001 by the Internet Fraud Complaint Centre (IFCC), is committed through Internet auctions (IFCC, 2001). In recent years, online auction sites have seen tremendous growth. Internet auction fraud is said to encompass things like non-delivery, misrepresentation, triangulation fee stacking, black market items, multiple bidding, and shill bidding, according to the IFCC's May 2001 investigation. This sort of fraud entails holding an auction for a product that in actuality does not exist, which is what is meant by "non-delivery." When the vendor deceives potential buyers, misrepresentation occurs. In essence, the seller provides bogus descriptions and terms for the things up for sale.

Triangulation entails the purchase of a good by the offender using fictitious bidder identities and payment information on an online auction website. The winning bidder and the online retailer are subsequently asked how they discovered the stolen goods. When a buyer makes repeated bids under various aliases for the same item, it is known as multiple bidding. Over 1.3 million transactions are thought to occur daily on online auction sites, according to the IFCC. Online auctions made up 78% of the top 10 Internet fraud types in 2000, making them the most common type of fraud, according to information published by Internet Fraud Watch. General merchandise sales rating follows with 10%. However, among the top ten cybercrimes reported to the IC3 in 2010, online auction fraud ranked eighth in terms of frequency of occurrence while product fraud came in at 14.4 percent (IC3, 2010).

2.6.4 Advance Fee Fraud

The aim of advanced fee fraud is also to quickly get sensitive financial information from victims, such as their account number and password. Advance fee fraud, sometimes known as the Nigeria "419" scam, is a frequent online scam involving Nigerians. The term "419" refers to the portion of the Nigerian Criminal Code that deals with fraud offenses, accusations, and punishments. The scam mails frequently claim to be from Nigeria, however this is usually untrue. South Africa, the Ivory Coast, and Togo are among the other West African nations with significant rates of advance fee fraud. Nigeria is singled out for an odd and absurd reason. Prior to this, it was done by fax, phone, or postal mail.

Smith (2007) contends that the scenarios these letters continue to portray have their roots in genuine plans executed by the military administrations of Nigeria in the 1980s and 1990s. Internet users have recently received emails announcing big winnings. These emails solicit a little upfront payment from the victim in exchange for a sizable share of a sizable sum of money that is promised to them. If the victim pays, the fraudster either creates a series of additional costs for the victim or just vanishes. It can occasionally take the form of lottery spam, in which scammers send out letters informing recipients they have won the lottery and that they must pay a fee before receiving their packages.

Advanced fee fraud seems to be the most recorded target for scammers, according to the Office of National Statistics in the United Kingdom (2013), rating 40%.

2.7 The Effects of Cyber Fraud to Victims and the development of the Country.

According to studies by Marsh (2004), Button, Lewis, and Tapley (2009), Cyber fraud victims experience pain that goes beyond monetary loss. Victims of Cyber fraud suffer emotional, psychological, and physical harm. Victims have occasionally killed themselves or self-inflicted harm. According to a 2009 study by Button, Lewis, and Tapley on 750 Cyber fraud victims in the United Kingdom, 68% of the victims reported intense feelings of anger, 45% said that their emotions were negatively impacted by the financial loss, 44% reported stress, and 37% noted effects on their psychological wellbeing.

Additionally, only a small number of the victims reported relationship difficulties, physical or mental health problems, or suicidal thoughts (Button, Lewis &Tapley, 2009). The aforementioned works investigated how Cyber fraud affects victims. On the other hand, it is important to examine the effects on the country, particularly in the regions where these fraudulent acts are committed. Despite this, there aren't many studies on the effects of Cyber fraud on nations or cultures.

Cyber fraud has cost the government and private companies a tremendous amount of money lost from foreign investment and international trades as a result of foreign investor anxiety and low trust in investing in and trading with the country (Boateng et al, 2011; Obosu, 2009; Oduro- Frimpong, 2011). The reputation of a nation is destroyed, in Burrell's opinion (2008), by Internet fraud. Other academics argue that Cyber fraud threatens the nation's future and causes "fear and panic" (Armstrong, 2011; Asamoah & Agyapong, 2011; Oduro- Frimpong, 2011). Not only that, but it also depletes human resources most of whom are children posing a threat to a country's ability to maintain peace and advance economically. Therefore, it can be deduced that Cyber fraud damages the peace and development of the country if peace and development reflect the scenario where the fundamental needs of human beings are supplied and society is free from fear and desire.

2.8 Legal Processes for Dealing with Cyber Fraud.

In Ghana, offenses involving the Internet are regulated by both common law and statutory laws. Cyber fraud was not controlled by any laws until 2008. Computer hacking was made illegal in 2008 by the Electronic Transactions Act (Act 772) and the Electronic Communication Acts (Acts 775).

As a result, police officers now have the jurisdiction to prosecute suspected cybercriminals. To advance electronic commerce, e-government services, and other information society services, legislation such as the Ghanaian Electronic Transactions Act, 2008 (Act 772), National Information Technology Agency Act, 2008 (Act 771), Data Protection Act, 2012 (Act 843), and some related provisions in the Criminal Code were all passed in 2008 and 2012. The Act establishes the legitimacy of digital data, digital signatures, and electronic transactions.

The Act's Sections 10, 11, and 14 establish rules for the management and preservation of vital databases and computer systems, as well as for the control of Public Key Infrastructure and Domain Names. Section one of the Acts also aims to promote cyber security by outlining the fundamentals of cyber deterrence.The Act places a focus on crimes and frauds committed in cyberspace or on the Internet and also gives law enforcement authorities several procedural tools regarding cyber security issues. The Electronic Transition Act of Ghana establishes legal prohibitions for certain behaviors on computers, electronic devices, and the internet. There is more discussion of a few of these behaviors. Numerous types of computer crimes and fraud start with unauthorized access (Kunz & Wilson, 2004). The Act specifies rules for the security of networks or computer systems that are essential to vital industries.

According to the Act, the Minister of Communications has the authority to declare a computer system or computer network to be a protected system by publishing a notice in the Gazette. After making such a declaration, the Minister is then able to grant written permission for access to a protected system. When a computer system or network is used directly in conjunction with or for the following purposes: security, identity, communication, international commerce, and emergency services, it is normally regarded and treated as a "protected computer" under section 55 of the Acts. Unauthorized use of a computer, computer system, or computer network is another type of computer crime that is forbidden by most states.

If someone attempts to gain access to “protected system” without the Minister of Communications' permission or secures access to one without authority, they may be held criminally liable under the Act. According to section 55 of the Act, the offender will be subject to a fine of no more than 5000 penalty units or to imprisonment for a term of no more than 10 years, or to both. A fine of no more than 10,000 penalty units, a term of imprisonment of no more than twenty years, or a combination of the two may be imposed on anyone who knowingly secure an unauthorized access to a computer in order to access information from a protected computer.

A new penalty is established under the Act for purposeful, unauthorized damage to a protected computer or the Internet. As a result, the Act's section 133, subsection 3, states that anyone who knowingly transmits a program, information, code, or command that damages a protected computer without authorization or with authorization that is greater than necessary will be subject to a fine of up to 10,000 penalty units, a term of imprisonment of up to 20 years, or both. The Act also establishes criminal penalties for those who gain unauthorized access to a computer system that contains financial information or information that concerns national security and interest. Therefore, a person who knowingly secures unauthorized access to a computer or accesses a computer beyond what is authorized and that computer contains information from a protected computer or financial records from a financial institution, a consumer reporting agency, or a department or agency of the government, or any information pertaining to the security of the Republic of Ghana will be subject to punishment upon conviction, including a fine of up to 10,000 penalty units, a sentence of up to twenty years in jail, or both (Electronic Transition Acts 775: 133/2). The Act also makes it unlawful to send consumers unsolicited electronic communications, such as emails promoting unauthorized goods or services.

However, the Criminal Code Act 29/60 Section 131 and its ancillary provisions continue to be relied upon by the Police as conventional crime laws on false pretense. Anyone who defrauds anyone by using a false pretense is guilty of a second-degree crime, according to Section 131 on defrauding by false pretense. A person is not subject to imprisonment for a term that may exceed ten years under the law's vague description of the punishment for second-degree felonies. The lighter penalties for crimes committed in violation of these rules typically do not prevent fraudsters from committing cyber offenses (Boateng et al, 2011). Certain cases don't back up the accusations made against the suspects under that law.

2.9 Empirical Studies

Sarre, Lau and Chang (2018) argued that early studies on cyber fraud focused on the drawing similarities between traditional and cyberspace crimes. These studies relied mainly on the traditional crime theories and data was collected from college students. The long and short is that the studies had little impact since criminal-based journals viewed their publications as not clear-cut criminal issues even though interesting. The proliferation of new media tools and technology and wide adoption of the technologies created the need to investigate cyber fraud. This was equally heightened by the fact that, the methodological deficiencies that marred the effectiveness of early studies on cyber fraud were also greatly addressed (Sarre, Lau & Chang, 2018). Even though the significant challenge for cyber fraud scholars is, the lack of official statistics on most forms of cyber fraud, Sarre, Lau and Chang (2018) observed that scholars studying cyber fraud collected primary data in innovative ways, such as by analyzing forum discussions, bulletin boards, and blogs, deploying honeypots, and developing field experiments.

Others used different sample populations rather than the college students. As the saying goes ‘necessity is the mother of invention,’ cyber fraud scholars found ways to develop the field to address the practical challenge confronting society cyber fraud.

In one of such studies, Kranenbarg, Holt and van Gelder (2017) observed that cyber fraud shared the similarity of traditional crime where victims are likely to be offenders. The authors conducted a comparative study to ascertain the relationship between victimization, offending and victimization-offending between cyber fraud and traditional crime. The authors purposely selected 535 respondents for the study. The study revealed that victimization has influence on the committing of cyber fraud. This means that cyber fraud was a way of revenging on people who have victimized an individual. Kranenbarg et al. (2017) associated it to lack of self of control as well as routine activities.

In another study, Gandhi (2012) explored the propensity of various cyber fraud forms in the India. The researcher found that cyber fraud such as online stalking, hacking, phishing and vishing were rampant in India. Cyber stalking is a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. It is an online harassment or abuse of an individual. Moreover, hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. From these two forms, there is a clear indication that privacy of people are on the line as far as cyber fraud is concerned.

Moreover, Gandhi (2012) defined phishing as the sending of unsolicited emails to customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Likewise, vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. With phishing and vishing, Gandhi (2012) showcased the economic threats of cyber fraud where people can be defrauded through illegal means using cyber technology.

Still on the scope of cyber fraud, Jain and Shrivastava (2014) argued that cyber fraud is changing everything. The authors pointed the fact that the nature and forms of cyber fraud is multifaceted cutting across all spheres of lives such as economic, social, political and technological. For instance, while cyber fraud such as viruses, worms and trojan horses, hacking and cracking affect efficiency of new media operation, other cyber fraud such as cyber stalking, cyber defamation, child pornography among others are distracting the social fabric of society.

Similarly, the emergence of vishing, phishing, financial crimes (credit card fraud, money laundering etc) are threatening the economic life of society. The complexity and the fast pace at which it evolves made Jain and Shrivastava (2014) to assert that law enforcement officials have been frustrated by the inability of legislators to keep cyber fraud legislation ahead of the fast-moving technological curve. The frustration of law enforcement agents in handling cyber fraud could be accounted to four factors identified by the US Department of Justice in a report (2001, p.23). These challenges are difficulty in finding evidence in the information ocean, anonymity of perpetrators, difficulty in traceability of perpetrators and the right of encryption.

These factors are vital areas of policy because with their presence, the handling of cyber fraud becomes complicated if not impossible. Gandhi (2012) also argued that the trans-national nature of some of the crimes require international collaboration in dealing with cyber fraud. In other words, offenders of cyber fraud could be different nationals hence dealing with such cases require international policy guidelines. However, such policy guideline is not yet available.

Exploring the effects, Saini, Rao and Panda (2012) found that there are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber-attacks. The attacks that are processed knowingly can be considered as cyber fraud and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. To the authors, restriction of cyber fraud is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. The researchers discovered that cyber fraud has huge impact on the companies as well as consumers. On companies, cyber fraud has created the need to spend huge sums of money in providing cyber security which can safeguard the companies' valuable online information from possible manipulation by hackers or crackers.

Moreover, it is discovered that consumers' trust for online transaction is dwindling because of cyber fraud. According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception that the Internet is rife with credit card fraud and security hazards is growing. There is the need for national security to tighten up in closing the cyber security gap between malign users and benign user of cyber space.

In terms of policy and cyber fraud, Adam and Berenblum (2019) discussed that there is the need for cyber fraud researches to explore the effectiveness of policy in combating cyber fraud. While the researchers commended criminologist and social scientist for delving into the relationship between traditional cyber fraud and cyber fraud using traditional crime theories such as routine activities theory, social learning theory among others, the researchers argued that the early works on cyber fraud were methodologically weak relying on college students for data with no reference to the policy component of combating cyber fraud.

Drawing from the glimpse of evidence that Howell, Burruss, Maimon, and Sahani (2019) provide on their maiden study on cyber fraud and policy, Adam and

Berenblum (2019) recommended the need for detail research in the area. In their study entitled *'Website Defacement and Routine Activities: Considering the Importance of Hackers' Valuations of Potential Targets,'* Howell, Burruss, Maimon, and Sahani (2019) examined the causes and correlates of website defacement at the macro-level.

They provided a rare examination into how structural characteristics are related to the frequency of website defacements at the national level. Collecting data on website defacements, Howell et al. (2019) used routine activities theory as a framework to find that website defacements were less likely to occur within a country that had capable guardianship and more likely to occur when target suitability was present.

These findings only applied to the frequency of recreational website defacement and not political website defacements. Howell et al. demonstrate that routine activities theory continues to be a useful framework to study cyber fraud, regardless of whether the test occurs at the individual or macro level. In short, the area of policy and cyber fraud mitigation is found to be effective in addressing the situation, there is little attention and empirical evidence on that perspective.

It is therefore vital for me to accept the critical observation of Dupont (2019), In his work entitled: 'Enhancing the Effectiveness of Cyber fraud Prevention through Policy Monitoring,' that countries around the world have spent massive sums to invest in cyber security, but have not spent the resources to develop tools to assess the effectiveness of government interventions in reducing cyber fraud. The sure security of nation is based on the effective collaboration of academia and policy makers to find working solutions to the cyber fraud.

In conclusion therefore, cyber fraud is an interdisciplinary area that requires all hands on desk, criminologists, social scientists, computer scientists, journalists among others to address the situation in a holistic manner. Moreover, policy making, especially national and international policies on cyberspace is key area that must be a joint work of academia and policy makers in order to bridge the information gap that leads to defective policies. As Gandhi (2012) rightly put it that future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters, but happen in cyberspace. Intelligence operations and covert actions will increasingly become cyber-based. It is important that our intelligence agencies gear themselves up to this new threat.

The same way Sarre, Lau and Chang (2018) foresaw the a great need for more academics to get involved in cyber fraud prevention and cyber security research because the work needs not only a criminological lens, but a multitude of lenses: legal, sociological, and political, in order for us to understand the impact of cyber fraud across the globe.

2.10 Theoretical Framework

This section is devoted to describing the theoretical foundations of Cyber fraud within which the implication of Cyber fraud can be analyzed. Routine Activity and Space Transition Theory are the two main theories used in this study. These led the foundations of the study because, they describe the motivational factors and behavioural patterns of Cyber fraud perpetrators. This helps to understand why perpetrators of Cyber fraud, do what they do, which is one of the study's objectives. However, none of the theory addressed the consequences of the perpetrators' behavioral style as a motivation for cyber fraud. They both argued on the factors that lead to Cyber fraud.

2.10.1 Routine Activity Theory

Routine activity theory, developed by Marcus Felson after being first proposed by Lawrence E. Cohen and Marcus Felson in 1979, is one of the most often cited and significant theoretical concepts in the area of criminology and crime research in general (Bennette, 1991; Felson, 2002; Nalla, 2014).

It is mostly used to present a macro-level view of cyber fraud. Unlike theories of criminality, which focus on the criminal and the psychological, biological, or social causes that drove the criminal act, routine activity emphasizes the study of crime as an event, emphasizing its link to space and time, as well as its environmental character and repercussions. (Broadhurst & Choo, 2009). According to the theory, persons' daily activities in a certain setting have an impact on offending behavior in that environment (Nalla, 2014). Routine activity theory is, in a summary, an attempt to uncover criminal activities and patterns at a macro level through the explanation of changes in crime rate trends (Cohen & Felson, 1979).

It is based on criminal events, rather than the search for offenders' motives, and thus provides a frame of reference for concrete and individualized crime analysis and facilitates the application of real policies and practices aimed at changing the necessary elements that make the existence of a crime possible and thus preventing it (Tilley, 2009).

As a result, some persons are more prone to being considered as ideal targets by a rationally calculated perpetrator due to the regularity of activities they engage in during their day and night lives. They derived two seemingly simple ideas with significant implications from this: first, that the opportunity for crime may be dependent on a configuration of distinct (though not disaggregated) elements of the aggressor or criminal; second, a correlate of the first, that the absence of either of the first two elements (aggressor and target) or the presence of the third (capable guardians) would be sufficient to prevent a potential criminal event. The notion is that psychological and social elements have only a minor part in an offender's decision to commit a crime in the immediate aftermath. The foundation of routine activity theory is that societal factors such as poverty, inequality, and unemployment have little impact on Internet fraud (Felson & Cohen, 1979). This theory describes the dynamics of criminal events patterns in criminal victimization and the prediction of victimization geographical elements that lead to crime when present (Pratt, Holtfreter & Reisig, 2012).

Cohen and Felson (1979) pointed out an important sociological paradox in their seminal article, "Social change and crime rate trends: A routine activity approach." They focused on changes in structural patterns of people's daily activity to explain this contradiction, focusing on how the new configuration provided more criminal opportunities and, as a result, could influence trends in rates of certain types of crime, particularly crimes against persons or property (Felson & Cohen, 1980). This theory describes the dynamics of criminal events patterns in criminal victimization and the prediction of victimization geographical elements that lead to crime when present (Pratt, Holtfreter & Reisig, 2012).

Three key conceptions evolve as a result of habitual actions that support or discourage criminal activity, according to Cohen and Felson (1979). The first is the presence of potential criminals and those who are looking for, willing to, and capable of committing crimes. Individuals who are not only capable but also willing to commit Internet fraud are known as motivated offenders. Second, the possession of a suitable target person or property that is unaffected by crime. A vulnerable or unusually appealing person or thing can be a suitable target for perpetrators (Pratt, Holtfreter, & Reisig, 2012).

Finally, there is a shortage of capable and willing guardians (lack of protection, devices, and techniques to battle offenses). The existence of capable guardians, according to the theory, deters persons from offending. The presence of guardians will deter the majority of offenders, making even the most appealing targets off limits. As a result, the availability of opportunity combined with the absence of guardianship raises criminal incentives, raising the risk of a crime being committed. Bennette (1991) stated that crime cannot arise without the convergence of these three conditions.

Many scholars have contributed to the theory's progress over the last three decades. The creation of Situational Crime Prevention is one of them (SCP). SCP concentrates on ways to make a feasible target less appealing (Felson, 1998). Felson's (1998) VIVA (Value, Inertia, Visibility, and Accessibility) model is used to determine the target's feasibility. The value a motivated offender places on a specific target is determined by the target's social and economic valuations, and higher-value targets are more appealing to offenders (Felson 1998).

Smaller, easier-to-carry objects, much as a smaller person is more likely to be victimized than a larger, more muscular one, may be more appealing to offenders (Felson 1996). Visibility influences an offender's decision because it informs them that a possible target is vulnerable; in order for an object to be targeted, the offender must be aware that it exists (Bennett 1991).

Finally, accessibility is thought to have a role in determining offending; Internet fraud is seen to be common due to the availability of simple 'pre-packaged' software (Broadhurst & Choo, 2009). Researchers argue that lowering a target's worth, visibility, and accessibility while increasing its inertia will deter offence (Cohen & Felson, 1979; Felson, 2002). The theory's research also backs up the situational nature of Cyber fraud and how certain "risky behaviors" increase the chances of becoming involved in violent scenarios. According to the hypothesis, if a person is in a dangerous environment or a disorderly neighborhood, he or she is more likely to engage in illegal activities such as Cyber fraud.

According to Chapple and Hope (2003), such chances encourages the youth to engage in criminal behavior. Surprisingly, the majority of criminal behavior appears to be impulsive, with little regard for the consequences. Victimization by violent crime and Cyber fraud both have the same underlying causal mechanism linked to the everyday actions of possible crime targets (Pratt, Holtfreter & Reisig, 2012). Situational and crime-specific factors contribute to the appeal of a particular target. It reveals who is more likely to become a victim. It is important to emphasize, however, that there is a link between crime victims and offenders, therefore patterns discovered by Routine Activity Theory may be misleading.

Furthermore, because crime rates are often related to the amount of motivated offenders in the population, such as teens and unemployed people, motivation can be reduced when lawful means for offenders to attain their goals are accessible.

When committing a crime is the only plausible alternative for an offender to fulfill their aims, motivation can rise. When attempting to understand 'the offender,' the Routine activity hypothesis has its limitations as well. That is, criminals cannot be understood just on the basis of their criminal activities, as rational profit-driven networks of criminal actors, because socio-cultural variables play a significant role in the formation and persistence of such groupings (Broadhurst & Choo, 2009).

The idea fails to recognize that the offender's moral convictions and socialization can influence the habitual activities that lead to crime. Even in the presence of criminal possibilities, offenders who have been socialized to embrace conventional views would refrain from committing crimes. The routine activities theory explains why and how youth, in particular, are at a higher risk of engaging in criminal behavior and being victimized.

However, there is a theoretical gap in that there is no relationship between motivational elements and the implication, which, when articulated, might readily be used to dissuade Cyber fraud. The idea thinks that guardianship is effective in deterring criminal activity, but when the consequences of criminal activity are not identified, guardianship becomes more of a temporary measure than a long-term solution.

2.10.1.1 Relevance of the theory to the work

The routine activity theory was relevant to the study because, it was used to examine crime from the perspective of the perpetrators. Crime would not be committed, according to the theory, unless a potential perpetrator believes the victim is a good fit and with the absence of a responsible guardian. Whether a crime will be committed depends on the offender's evaluation of the circumstances.

2.10.2 Space Transition Theory

K. Jaishankar developed the space transition theory in 2008. The idea is one of the most significant theoretical formulations in criminological literature and, in cyber criminology, one of the most often mentioned theories today. This theory sees the rise of cyberspace as a new hotspot for criminal activity and explains how crimes in cyberspace are caused (Jaishankar, 2008). The growth of cybercrime theories was influenced greatly by the development of the space transition model. That is because it was issued at a time when no other social scientist had been able to fully describe the general phenomenon of cybercrime as well as Jaishankar. The notion was first published as a chapter in the book "Crimes of the Internet," which was published by Prentice Hall (2008, pp. 283-301). There have been several since then. The theory's utility will be tested through empirical research. Some academics have a high regard for others have praised Jaishankar's ideas for combating cybercrime, while others have condemned them. A handful of his theory's premises are difficult to evaluate and may be unique to certain situations.

In that, as in the case of Ghana, Space Transition Theory is informative to the study of Cyber fraud (Danquah & Longe, 2011 cited in Warner, 2011). Because identity flexibility, dissociative anonymity, and a lack of deterrence factor in online offer offenders with the choice to perpetrate Cyber fraud, this theory appropriately assesses that a person has the predisposition to do crime in cyberspace that they would not commit in physical space (Jainshankar, 2007 p.7). "The nature of people's conforming and non-conforming behavior in physical and cyber space is explained by space transition theory.

The transfer of a person from one space to another (for example, from physical space to cyber space and vice versa) is referred to as space transition. People behave differently as they go from one space to another, according to the space transition theory (Jaishankar, 2008).

This theory proposes that people who have repressed criminal behavior (in physical space) are more likely to commit crime in cyberspace than they would in physical space due to their status and position. Also, in cyberspace, identity flexibility, dissociative anonymity, and a lack of disincentive element offer criminals with the option of committing cybercrime (Jaishankar, 2008).

Furthermore, the idea predicts that criminal activity of criminals in cyberspace is likely to be imported to physical space that, in physical space may be exported to cyberspace as well. Strangers are more likely to band together in cyberspace to commit crime in physical space, whereas physical space associates are more likely to band together in cyberspace to commit crime.

Advances in information and communications technology (ICT) have introduced a variety of new crime challenges, according to Smith (2002), but they have also made crime prevention, detection, investigation, prosecution, and punishment easier. The space transition theory' emphasizes that a clash of physical space norms and values with online norms and values can lead to cyber fraud.

As a result, the goal of this study is to empirically evaluate the Space Transition Theory to see if it can be used to predict cybercriminal motivational factors. The theory, on the other hand, falls short of explaining why people who would not commit a crime in physical space engage in Cyber fraud in cyberspace. When these factors are identified, stronger policies to prevent Cyber fraud can be enacted.

2.10.2.1 Relevance of the Theory to the work.

As a method of character analysis for offenders, the space transition theory was useful to the study. It was stated in it that: persons, with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position. Also, Criminal activity by perpetrators in cyberspace is likely to be imported into physical space which, in physical space may be exported to cyberspace as well.

2.11 Chapter Summary

This chapter focused on new media and cyber fraud. It also, establish the prevalence, forms of cyber fraud and Grabosky's Classification and existing literature in the area of cyber fraud. Also, this study is grounded on Routine activity theory which is based on the assumption that crime can be committed by anyone who has the opportunity and Space transition theory that also argues that, people behave differently when they move from one space to another. Based on this assumptions the concept, practices and the effects of cyber fraud on the country was looked at. Legal processes for dealing with cyber fraud was also dealt with and Researchers' studies examined as empirical proof for the work which concludes with a summary of the study's conceptual frameworks. The next chapter discusses the data collection methodology and analysis.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter presents the study methods in depth. The various techniques and methods for selecting respondents to take part in the research was discussed. The chapter presents the research approach, research design, sampling and sampling technique, sources of data, data collection instruments, data processing and analysis, Ethical considerations, field entry processes and field issues.

3.1 Research Approach

The study was conducted using a qualitative design. According to Lindlof and Taylor (2002), qualitative studies are grounded on social practices and meanings of people in a specific historical or cultural context.

Qualitative data are in the form of texts, symbols or phrases (Kreuger & Neuman, 2006). For this reason, this study employs the qualitative method since it seeks to investigate the scope of cyber fraud among perpetrators, factors that motivate the youth to engage in cyber fraud which are all real-life situation.

Qualitative research enables social science researchers to study a particular phenomenon or culture because it gives room for flexibility and the attainment of a deeper understanding of the subject or phenomenon (Yin, 1998). Qualitative researchers are focused on understanding the meaning people have constructed, and their experiences. This perspective is relevant to the study because the research involves the perspective of the youth about curbing cyber fraud among the youth in Ghana and the implications of the discourse on the phenomenon being studied.

Data were collected from multiple and triangulated sources including Face-to-Face interview, mobile phone call recordings, general online research among others and making interpretations of the meaning of the data (Cresswell, 2014).

The study, on the other hand, takes a descriptive and exploratory method. (Cooper and Schinder,2011) described descriptive research as involving the gathering of data, describing the phenomenon, organizing, tabulating, depicting and describing data collection in the form of graphs and charts in order to help the reader understand the distributing data.

The descriptive approach was chosen because it provides a descriptive account of an individual's perception, viewpoints, and attitude toward events or an object (Hakim, 2000). This research design is appropriate for investigating the scope and factors of cyber fraud participants. Furthermore, an empirical evaluation of a few studies makes it necessary to describe the many characteristics of Cyber fraud, such as its prevalence, forms, and classifications according to “Grabosky”.

The exploratory method was also utilized to gain a better understanding of the theological perspective such as the routine activity and space transition theory. This lead to further explanation of the concept, practices and legal processes for dealing with cyber fraud. Because cyber fraud is socially constructed, it is impossible to independently verify one's understanding of it and its implications. The difficulties that underpin cyber fraud are frequently context-specific, revealing the perspectives of those engaged. Their thoughts on cyber fraud and its implications are also expressed in their perceptions. These do not fit into a quantitative research methodology. As a result, descriptive and exploratory approaches are appropriate for this study, which intends to sample the perspectives of participants and other important informants on the consequences of cyber fraud in the research area.

3.2 Research design

According to Creswell (2014), research designs are types of inquiry within qualitative, quantitative, and mixed methods approaches that provide specific direction for procedures in a research design. After choosing a research approach for a study, it is important to consider the mode of inquiry within the approach selected to serve as a framework for exploring the research findings (Sileyew, 2019). Denzin and Lincoln (2011) refer to research design as strategies of inquiry. A research design is a detailed plan or method for obtaining data scientifically (Schaefer, 2004). Saunders (2007) defines research design as the general plan of how the research questions would be answered.

The selection of an appropriate design depends on the nature of the research, the research problem and questions, personal experiences of the researcher, and the type of audience for the study (Creswell, 2014). Research designs, especially in the qualitative sense, generally comprise narrative research, phenomenology, qualitative content analysis and ethnography and many others. The study used the narrative approach as the method of inquiry for this study.

3.3 Sampling and Sample Technique

The main technique used to pick the respondents for the study was non-probability sampling. The study employed a combination of snowball and purposive sampling techniques. The selection of participants was based on snowball sampling.

This was repeated until the desired sample size was achieved. Purposive sampling was also used to get data from people who were relevant to the study. Individual characters among the participants were picked to respond to questions about the scope of cyber fraud among perpetrators, factors that motivate the youth to engage in cyber fraud and the perspective of the youth about curbing cyber fraud among the youth in Ghana.

A total of 10 participants were selected using my personal network and the internal feedback I had gotten from each participant after requesting them to take part in an interview for a project. Five respondents were randomly selected from a department at each institution, (Wisconson International University and Academic City University). The 10 respondents from the two tertiary institutions were then questioned.

3.4 Data Collection Models

Interviews were used to acquire data for this qualitative study. The interviews were done using an interview guide that had been created in advance by the researcher. The interview was semi-structured and straight forward. This was done to provide flexibility and to aid in the gathering of even unforeseen information. An interview guide was used to interview 10 students. The interview guide's questions reflected the study's aims.

The interview was conducted at the respondents' convenience. The researcher used a voice recording device to record the responses, as well as taking handwritten notes. With the help of an observation check-list, extra data was collected outside of the interview. In this study, non-participant observation was utilized to monitor the environment, attitudes, and actions of participants.

As a result, the activities and informal discussions with respondents were monitored, in order to understand the activities of the alleged perpetrators. In the field handwritten book, information gathered during the observation process was recorded in the form of informal talks, personal reflections, and analysis. Data was collected during a two-month period.

3.5 Data Analysis

Thematic analysis is a type of qualitative analysis used to find, examine, and describe patterns (themes) in data. It is employed to examine classifications and present themes (patterns) related to the data (Boyatzis, 1998). Code and theme are terms that are used interchangeably in Boyatzis' (1998) theory of thematic analysis. A theme is a particular pattern in the data that is of interest. Miles and Huberman (1994) claim that the process entails coding, categorization, and pattern-noting in order to establish a connection between the variables and components in order to produce an acceptable and logical chain of evidence.

According to Marks and Yardley (2004), thematic analysis is thought to be the most suitable for any study that aims to discover concepts and ideas and interpretively depict human behavior. It adds a systematic element to data analysis. It enables the researcher to relate a frequency analysis of a theme to one of the entire contents. Therefore, thematic analysis was adopted to derive themes from the gathered data. This was only done based on the in-person interview.

I coded for the various types of cyber fraud that the participants were engaging in for Research Question 1, which highlighted the scope of cyber fraud. I also coded the act's execution. Come and marry me, Military format, Gold format, Construction or Agricultural format, and Carding are some of the themes that were derived from the findings. I drew meaning and interpretations from the data by applying concepts and theories from my theoretical framework to the findings. The interpretations and discussions were further supported by direct quotes from the participants. Data were double-checked and revised to ensure that responses were correct and free of errors. Data acquired with an electronic recorder was transcribed and presented in themes that emerged from the interviews in accordance to the study's objectives. After that, the themes were narrated. On the prepared field notes, which contain a lot of information, manual sorting was done.

3.6 Ethical Considerations

Because this study involves human subjects, it is critical that ethical norms be followed carefully and severely. Respondents were made aware of the research's goal in order to protect their rights when answering the questions. The respondents' privacy and confidentiality were safeguarded, and the information gathered was utilized only for the indicated purposes.

3.7 Data Collection Processes

The researcher used a number of procedures to obtain correct data from the respondents while also ensuring that it did not contradict with study ethics. A close friend linked the researcher to group of students involved in such activities on campus. These students consented to respond to questions after multiple persuasions and explanations of the study's goal, as well as to persuade others to respond to questions that will be asked. The Researcher guaranteed participants of the confidentiality of every response made which is only for academic purposes. The participants set up a suitable time and day with each participant so that the researchers could receive a briefing on the procedures of the research topic and its activities. This hour-long one-on-one interview with participants took place over the course of a week. As a result, questionnaires were created based on the research questions and sent to them before the interview day.

3.8 Chapter Summary

This chapter provides a comprehensive process and procedure for data collection and analysis. The study, which is qualitative used a descriptive and explorative approach. Using a coding sheet, data were exclusively gathered using qualitative descriptive and explorative methods. Thematic data collection approach was used to analyze the information obtained. The analysis of the data gathered is presented in the next chapter, along with a discussion of the findings.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.0 Introduction

This chapter comprises discussions on the study's findings. The issues covered involved the scope of cyber fraud to enable readers to get the basic understanding of cyber fraud and it forms in order to explain the factors that motivate the youth to engage in it: The chapter presented detailed discussions of findings from data collected using the methods specified in the previous chapter. Along with relevant theories and related literature, the study brought out the key issues regarding the factors that motivate the youth in engaging in cyber fraud, the participants' perspective about curbing cyber fraud among the youth in Ghana and the legal processes for dealing with the issue. For easy analysis and interpretation, the data derived was simplified into several thematic units which were thoroughly described and critically analyzed.

4.1. What is the Scope of Cyber Fraud among Perpetrators?

The scope of cyber fraud in this literature refers to the several types of cyber fraud that exist within the internet domain. This has been a similarly perplexing issue in terms of the breadth of cyber fraud. Cyber fraud encompasses a wide range of unlawful activities. As a result, there appears to be some misunderstanding about what is being discussed when cyber-fraud is brought up.

Cyber Fraud can include things like fraud, technology theft, security breaches, identity theft, child pornography, and stalking. Even within the computing community, there appears to be significant dispute over what constitutes criminal action. Some contend that some types of hacking, such as breaching and maybe altering a secure computer system, should never be considered a criminal crime.

The advantage of this typology is that it divides offenses into two categories: those oriented toward technology (Type I offenses) and those oriented toward humans (Type II offenses) (Type II offenses). Some crimes will be almost entirely technological in character, while others will be more traditional crimes that will be made easier by computers. As additional types of computer-related crime arise throughout time, this typology will allow for continued extension. The following are the various responses from participants. This constitute 80% of the responded sample size of the research and it gave out almost the same or similar feedback. The question that leads to the scope of cyber fraud and how it is perpetuated was pose to them.

4.1.2. Confidence / Romance Fraud (Come and Marry Me)

According to the respondents in the interview, the most popular sort of fraud is the confidence/romance fraud, often known as "***come and marry me***" in the scamming world. It is a relatively new type of fraud that first surfaced about 2008. The respondent claimed they pretend and establish a relationship with their victims through online dating sites, then scam them of substantial quantities of money.

Despite its newness, it is estimated that 230,000 Britons have been victims of this crime. The scam, which first surfaced in 2008, is based on a paper-mail scam in which participant pose as a romantic partner on online dating services and then rob their victims of substantial sums of money. Victims of this crime suffer a 'double blow,' as they lose both money and a relationship. Confidence/romance fraud occurs when an actor deceives a victim into believing they have a trust relationship, whether family, friendly, business or romantic and leverages the relationship to persuade the victim to send money, provide personal and financial information, or purchase items of value for the actor, Federal Bureau of Investigation (FBI, 2022).

This fraud comes in various forms which includes, Romance, Business partners in either Gold, Construction or Agriculture sector. In some cases, the victim is persuaded to launder money on behalf of the actor. The scams are interconnected, so if you participate in one, you may simply be able to engage in the others as long as you have documents to prove your authenticity to your victims. Respondent claim to the use of online dating sites to pose as U.S. citizens located in a foreign country where they intend to scam.

A respondent indicated that:

> *"With this type, you only pretend to love the victim and lure him to believe that there is a relationship between the two of you or there can be some love relationship between the two of you. With this, you chat him in a romantic manner and then you tell him all sort of things to let him know you are in love with him and what to build a life with him. You just have to convince him. That's all".*

One can opt to chat exclusively with female or male victims in this scam. When a scammer decides to talk with women, he or she is either engaging in one of the other forms of confidence romance hscams, such as military, gold, construction, or agriculture. The scam is dubbed "come and marry me" because the fraudster wants the victims to believe they want them to come to Africa and marry them. The scam's victims are predominantly men, and the majority of them are in their late seventies. The majority of con men who have defrauded their victims of large sums of money have succeeded in relocating female relatives or friends to the United States or the United Kingdom.

This is because most elderly men who have been conned do not want to lose anything, so they agree to accept the scammer's sister or female friend, but only if the person is interested in marrying a white person.

According to the interview, scammers must first sign up for a dating site where they can meet their potential victims. eharmony.com, match.com, ourtime.com, zoosk.com, elitesingles.com, cupid.com, and badoo.com are just a few of these dating sites available. According to the interview, getting registered on any of these dating sites is one of the most challenging aspects of their scamming job, and most of the fraudsters use experts who are also into site payments.

This group of experts, dubbed "carders," are also fraudsters, but their focus is solely on using stolen credit cards from victims or businesses to make payments to these websites, allowing confidence romance scammers to register with false information and chat with genuine people who are on the online dating site looking for a soul mate. Before they will accept to pay for you to be able to talk with your possible victims on any of these dating sites, the fraudsters pay instant cash in cedis to these "carders" through either MTN momo or any of the other networks.

According to the Respondents, finding a trustworthy carder is sometimes a problem because they are also conned if they do not find a legitimate person. As a result, the majority of them choose "carders" who are referred to them by their peers. Every transaction is done electronically through Momo, and the carders never meet you face to face. Once you have found a reliable "carder," you are halfway to becoming a successful confidence/romance scammer. This is because if you gain access to any of these dating sites, you will have the possibility to meet highly wealthy victims from other countries who are looking for a soul mate with whom they can spend the rest of their lives. During the interview, it was discovered that scamming is not just easy as perceived by those who are not involved in it, but that the participants themselves invest a significant amount of money to obtain what they refer to as "tools."

According to them, these "tools" are highly expensive, and even if you have the money, how to obtain it becomes a problem; either you are scammed in the process of scamming, or you won't be able to do it at all because everyone who sells the tools does so anonymously. As a result, if you do not want to risk losing money by sending to an unknown person, you cannot even begin. Once you have been conned a few times, it will either urge you to be more cautious or discourage you from continuing. They identified some of the important technologies that help them work, such as a VPN (Virtue Private Network) that allows them to mask their present location and change it to the country where they need to communicate from. You would not be able to access most web sites without a very strong VPN, especially the more restricted and highly secured ones.

Socks was also mentioned, and it operates similarly to VPNs and accomplishes the same goals, with the exception that it protects the scammers' anonymity. As a result, they merged the two. Once you have these two items, you may sign up for any online dating site you choose, and once you find a "carder" to pay the dating site for you, you are ready to go. The next thing you will need is a document, which they can also get from anonymous websites. Participants impersonate genuine victims who are on online dating services looking for a potential soul partner. So they send winks to random victims, who either wink back or react with a message. This gives them both the opportunity to strike up a conversation.

The participants said that most of them are experts because they have been doing it for years, so when the victims respond with a wink, they take advantage of the opportunity to obtain their victims' email address or phone number. This is because most online dating sites have security mechanisms in place and may remove scammers from the site if they identify that you are a fraudster, so they don't waste time on unimportant matters. They get right to the point and focus on getting their victim off the online dating site and into a location where there are no security measures in place to track them. Once both of them have introduced themselves, the scammers tell the victims who they are, what they do for a living, and what brought them to the website.

They usually appear to be quite wealthy, which allows them to easily persuade their victims to accept them since they believe they are genuine. With that quick introduction, both of them are convinced, and the scammer tells the victim that they should both leave the online site because he believes they are soul mates who were brought together by divine intervention, and that they should either continue their conversation via email or text via the phone number. This is done to circumvent any security measures on the online platforms that record their discussions and can be used to track them down on the website obstructing their operation.

The entire process begins once they have successfully taken their intended victim from the online dating site. The respondents explained this as to reasons why fraudsters are generally spotted awake late at night browsing and they explained this was due to the time differences, as they pretended to be citizens of the United States, the United Kingdom, or Europe on the online platform. In order to persuade their potential victims, they did not need to sleep from 12:00 a.m. to 5:00 a.m. local time because that is the time that their potential victims are awake in their country, and most of the victims can only chat with you when they return from work. To attain their aim, they must persevere and sacrifice their sleep.

When I tried to find out how they communicate with phone numbers via text messages, they revealed that they buy foreign phone numbers online with the help of "carders." You pay a "'carder" locally through Momo, and the person purchases the phone number of the country you wish to appear to be conversing from, which may be the United States, the United Kingdom, or any other European country. They send a lengthy, well-written introduction to themselves during the early days of interacting on the newly constructed and secured site, which is either through emailing or texting their victims' phone numbers.

They claimed to begin by thanking the potential victim for the opportunity to connect on a secure platform, as well as praising God for enabling them to meet, as the participant understands why God brought them together. They have a religious appearance, which allows them to gain a lot of trust from their victims. They then proceed to inform the victim about themselves and their families in detail.

The introduction focuses entirely on the orphanage with the phrase "come and marry me." The fraudster creates a thorough account of her family. Depending on where the victim is from, her father could be from the United States or the United Kingdom. They tell you that their father was a very wealthy man from the country where you, the victim, is from, but he died in an accident or from an illness a few years ago, but their mother is an African, and that they are chatting from Ghana. They tell you that after losing their father, who was their rock and everything in their lives, they went to Africa for the first time to learn about their roots.

Their story continues until they tell the victim how, after their father died, they lost their mother and, as the only daughter in the family, they were obliged to continue their stay in that country for a period of time. They inform you that they are currently enrolled in university and taking a nursing course before telling you about the gold or agriculture narrative. They will ask you to buy them an iPhone in a month or two into the conversation to see how well you have earned their confidence. Once you purchase the iPhone, they will take you serious and start telling you additional stories in order to extract more money from you.

All of this information aids them in defrauding you once they demand money. Those who engage in this type of deception, known as "come and marry me," can simply transition to the military, gold format, construction or agriculture. The format for those stories is based on the story they tell you in the “come and marry me”. They will transition and take you to the other forms, which are on a business level, once they have deceived you for years and you stop paying them money. They inform the victim about their deceased parents' property, which is gold or agriculture, which they traded while alive.

4.1.3. Military Format

This form of scam is similar to the confidence romance scam, however the participants converse as men while the targeted victims are all women. Furthermore, in this sort of confidence romance scam, the fraudster always poses as a service personnel from the United States or the United Kingdom.

According to the respondent, this form of romance scam is the most hardest to pull off, and you will need to be an expert as well as very knowledgeable to be able to practice because you will need to present a lot of documentation when it comes to the end of the hoax.

During the early days of conversing on the newly established and protected site, which is either through emailing or texting their victims' phone numbers, They send a lengthy introduction to themselves, which is well-written. It begins by thanking the potential victim for the opportunity to communicate on a safe platform, as well as thanking God for allowing both of them to meet because the scammer knows why God brought them together. They appear to be religious, which allows them to garner a lot of confidence from their victims. They then proceed to tell the victim a good part about themselves and their families. This is the part where they talk about their job, family, and money. To keep their victim consoled, they usually relate a story about their lost lover, whether it was due to an accident or an illness.

They tell their victim that they have been looking for a life mate since their partner died, and that they believe God has finally answered their plea. They tell their victim about their son, who is staying at a boarding home with a caretaker. When their victim reads their message or text, she becomes more convinced and also opens up. As a result, the entire detail about them must be included in the first message to serve as a cornerstone on which all subsequent talks will be built.

As a result, individuals who are not professionals seek the assistance of experts who have been involved in fraud for years to assist them in carrying out the work so that the money collected from the victim is divided, with the experts receiving 60% and the victim's owner receiving 40%. The majority of the experts are extremely wealthy individuals who have amassed their wealth by deception and have gold and most of the documents in their possession. This is why they are brought in to assist, and because many of them have connections, a third person is brought in to masquerade as the actual acclaimed military person.

This third person is indeed white, but he is also a con artist looking for a business and his cut. As a result, he receives his part as well, but from the experts' 60 percent. Every other technique and tool used to obtain the victim from the dating site are the same as in the confidence romance scam, except here the fraudster only chats with females.

The scammers pose as U.S. military members deployed overseas where there is an ongoing instability, example, Afghanistan, Iraq etc. A scammer may claim to be a service person who is deployed and is looking for a wboman to spend the rest of his or her life with. They come in for friendship but will send you messages about relationships, friendship, and other things on a daily basis and also pretend to be very good. Once both of you share locations of where you live, some can start buying you flowers, rings, phones, and other items as gifts in order to win your heart in the shortest possible time so they can start demanding money. They normally plan ahead of time, so they have photographs of the military personnel they claim to be.

One of the respondents mentioned that:

> *"For this type, you have to prepare very well because if you don't take care you will make a mistake and the client or victim will detect it. Once she detects it, she will just cut you off. Before, you engage in this, you have to find enough photos of the military man you intend to impersonate. Apart from ones that he is in the military uniform, you need the ones that he is in a usual wear as well because the military man cannot always be in a uniform. They go to Google and look up a certain military member's name, then download all of his photos and occasionally short recorded films. They exchange pictures with their victim and inform them that they have a child whose mother died in an accident and that the child is in boarding school due to their military service. This story about their child that they tell the victim encourages them to begin requesting assistance from the victim. They may ask you*

> *to give money to the caretaker of their ward in order to assist with his upkeep; they will repay you once they return home; they are not allowed to have money on them owing to their circumstances".*

4.1.4 Gold Format

This format builds on the "come and marry me" basis in order to defraud the victim. This format's whole introduction section is similar to the "come and marry me" approach. In this form of con, the fraudster tells the victim about a gold inheritance she received from her father, who had invested in a mining company in Ghana, where her mother is from. She gives you gold company documents and photos of herself, which are frequently photoshopped photos of her in a mining company photo. She displays a plethora of photographs and documents in order to persuade you to believe her. There have also been occasions when they have been able to edit video of the image she claims to be her in the video, and they have software that allows you to call her on a video call so that you can see her physically and believe what she is saying. When you call her, the software assists in showing the victim the recorded video, which he will believe is the true person he has met as love. In other cases, she will show you a gold bar in the video, which increases the victim's trust and desire to do business with them. Because it is being edited, the video normally does not have sound and the quality is a little low. They would inform the victim that the country from where they are communicating has a bad network. They engage the victim through video for roughly four times over the course of a month. They would not show you any more videos of themselves because they have gained the victims' trust by then.

What they generally do from here is present you documents based on what they want you to do; for example, they may tell you that it is a great business and that you should invest in it. Once you have decided to invest in it, you will start paying money to them using Western Union using an information they will give in their name. They will claim that the account holder's name is the agent that assists them with gold investments, but they are the ones.

One respondents mentioned that:

> *"For this type, they pose to be half American and half the country they claimed to be chatting from. In other terms, their mother from Ghana and their father an America. This is done so that it makes it easy for them to tell you they are currently in Ghana to visit their family without any problem. Once this story is accepted then they go on and on and on creating different stories just to defraud the client".*

They will continue to defraud you by taking all of your money till your money is finished, with the documentation and more proof of recorded videos they send you. Some of the victims will have to go to the bank for loans in order to come and invest in this gold business, which is a scam that will never yield any results. When you are unable to send them money again, they will stop communicating with you and the conversation will come to an end.

4.1.5: Construction / Agriculture Format

As previously indicated in the confidence/romance scam, the construction or agriculture format is built on the "come and marry me" foundation to defraud its victims. After you believe all of the stories that the scammer tells you throughout the come and marry me stage, the scammer takes your money. When he realizes the victim he is conversing with is a wealthy individual, he will automatically switch to one of these two formats.

In the early phases of the fraud, the scammer is able to discover this through their interactions. The scammer selects the next stage he will take the victim through once you stop paying him money during the early phases of the "come and marry me" scam. This is determined by the document in the fraudster's possession. If he has a lot of agricultural farming documents, that's where he will direct all of his conversations. The fraudster posing as a woman will tell you a similar story about her family as the gold format, but will also tell you that her father made a huge investment in agriculture, which includes both animal and large crop farming. The scammer selects the next stage he will take the victim through once you stop paying him money during the early phases of the "come and marry me" scam.

One of the respondents mentioned that:

> *"For this type, They claim to be having huge plantation of farms in Africa and therefore tell the clients a lot of good stories in the kind of business just to make it easy for them when they start to ask for money. In the course of the communication as time passes by, they start demanding money to buy more current equipment to aid the farming. Because the client has already heard good stories about the business, they quickly jump into it and start giving money as business partners"/*

This is determined by the document in the fraudster's possession. If he has a lot of agricultural farming documents, that's where he'll direct all of his conversations. The fraudster posing as a woman will tell you a similar story about her family as the gold format, but will also tell you that her father made a huge investment in agriculture, which includes both animal and large crop farming. She does so until he runs out of money, at which point she may ask him to go to the bank for a loan. All of this is contingent on the business's discussion line.

4.1.6. Credit card, Online Account and Online Shopping Scams (Carding)

Because they all involve the exploitation of victims' credit card information, credit card, online account, and online shopping frauds are all linked. According to the interview, this form of fraud plays a key part in the scamming society, and without it, scamming could have been reduced. The fraudster refers to them as "Carders," and their work is done in secret. As a result, the majority of scammers who engage in fraud are unaware of the majority of these "Carders."

They strike a deal with you, and you pay them in local currency, which is MTN momo. The majority of them also accept payment via bitcoin wallet, which is far safer for them than using a telecoms momo. According to them, to be a carder, you must be an excellent learner and observer, as carding includes a lot of reading of "tuts," or tutorials. To be able to engage in carding, you must have all of your tools ready. They define "tools" as the numerous technologies that assist them in doing their tasks. They buy the tools from anonymous websites on the internet. VPN, socks 5, RDP, and credit cards are some of the tools they utilize.

All transactions done online on those anonymous websites, according to them, including Yale Lodge Card Shop, CVV Union Card Shop, Real and Rare Card Shop, SwipeStore Card Shop, Valid Dumps, CC2BTC Card Shop, Big Money Card Shop, UniCC, Trump's Dumps, and others. Any "tool" they require can be purchased from one of these online shops, and all transactions are performed in bitcoin currency. Once they have all of the necessary tools, they go to websites that sell people's stolen credit cards and purchase them with bitcoin. They then proceed to accomplish what they intend to do, such as paying for an online dating service so that another fraudster can gain access and masquerade as a legitimate person in order to swindle victims.

They build a profile on a specific website, such as eharmony.com, millionairematch.com, seniormatch.com, elitesingles.com, jdate.com, match.com, or christianmingle.com. They pay for the website's services using stolen credit card information obtained from such anonymous websites. They transfer the login details to the scammer after they pay the online dating site to gain access to the website. If they wish to buy a product such as an iPhone, an electronic automobile, or any other valued thing, they go to the product's website and follow the same steps as before to complete the transaction.

The interviewer tried to find out how the fraudsters obtain products if they buy them from online shops in the United States, the United Kingdom, or Europe, and they made it perfectly clear that they usually had accomplices abroad. They don't know these folks in real life, but they meet them online in anonymous computer chat groups. So they believe that it is trust that binds them together because they do not know the other party for whom they are purchasing in the United States, the United Kingdom, or Europe, and all they can do is risk. When a person is honest, they immediately become business partners and collaborate on a shared basis.

A respondent mentioned that:

> *"If someone defrauds them, they keep looking until they find a real person to work with. With the online account, fraudsters go to an online bank services website and generate account information after purchasing the credit card information of a victim from those anonymous websites. The bank sends them information using the foreign phone number they purchased online once the account information is ready to use. They can then use that bank account to engage in commerce by putting funds into the account using the credit card information they purchased. Once money has been deposited into the victim's account whose credit card information has been stolen. The transfer takes effect, and they then transfer the funds to the other party, who is based in the United States, the United Kingdom, or Europe, so that he can withdraw and send their percentage back to them in Ghana".*

It was noted that, they have additional websites where you may verify and check whether the credit card you're buying from an internet website is active and has funds on it. When they check the card and see that there is money on it, they can use the card information to buy whatever they want until the money runs out.

4.2. What Factors Motivate the Youth To Engage in Cyber Fraud?

Information on the driving elements for university students' engagement in cyber fraud was also sought in order to better understand the situational and contextual indices that influenced their decisions to engage in this type of criminal activity. Different push and pull reasons accounted for respondents' involvement in cyber fraud, according to the findings. Only a handful of the students interviewed who were alleged practitioners of cyber fraud related their engagement in the criminal conduct to a desire for fun and amusement, while nearly all of them linked their reason for engaging in online fraud to financial need and peer pressure. Below are the themes that came out from the questions posed.

4.2.1. The Need to Make Money.

One of the primary motivations for perpetrators to engage in cyber fraud was financial gain. Cyber fraudsters are always on the lookout for easy ways to earn a lot of money. Multinational corporations and wealthy people who have access to a limitless amount of secret information are their primary targets. If we think about it, anything that connects us to the internet puts us at risk of cyber-attacks. One of the interviewees at Wisconsin University expressed his motivations for engaging in cyber fraud as follows:

> *To become rich and be self-dependent. Young people becoming rich day in and day out motives me and gives me hope that I can also become very very rich. (Interviewee 1)*

In the words of another:

> *My motivation to enter into such business is to make money since the system in Ghana here doesn't really help young graduate in acquiring a well-deserved paying job easily and also money must be made through different means and the safest and best way to do that was through online money making. (Interviewee 2)*

Also, a respondent stated:

> *It help solves my financial problems. It is also smart way to make money but not easy way because if it was easy anyone can do it and I wouldn't be limited. (Interviewee 3)*

Another had this to say:

> *My incentive for getting into cyber fraud is that it is simple to generate money without having to go to an office in the morning; I can make a lot of money from the comfort of my own home. It is a savior in disguise, and I believe that life would have been much more difficult for the youth without it.*

This means that the motivation behind engaging in cyber fraud is to become rich. They however, found cyber fraud as the shortest and easiest way to make money and become rich suddenly. As one of the respondent remarked, young people are becoming rich every day. Likewise, the interviewee 3 asserted that the motivation behind cyber fraud is that it helps in solving his financial problems. These problems are requiring money to resolve and cyber fraud is the clear source to meet those needs. The interviewee considered cyber fraud as a smart way to make money without limitation.

4.2.2. Unemployment

Almost every interviewee stated that unemployment is a key contributor to the problem of cyber fraud. In an interview, when the question such as, "What do you think are the suggested solution in curbing cybercrime?" was posed? The interviewees had the following to say:

> *There should be enough of employment for young people to do, and politicians should quit fooling us. They must pay us what we are worth for the work we perform. If this is done, the majority of us will be able to return to legitimate work and halt the cybercrime.*

In the words of another:

> *Because we practice and are also experts who are deeply into this business, taking us off the cyber Terence is completely impossible, but*

> *providing an environment whereby the knowledge acquired in making money online can be transferred or advanced into the business world to make more money in cyber operations is the best solution to these cyber frauds. I believe it would not address the entire problem, but it would at least keep the majority of the participants employed in the same position, or in a legal manner this time.*

Also, a respondent stated**:**

> *Job creation for the youth. Most of us find something to do due to a lack of employment; if jobs were accessible once we finished school, most of us would not engage in something like cyber fraud since we realize it is not a good thing to do. If there was jobs right after national service to engage a quantum number of graduates, the rate at which youth involve themselves into fraud would have reduced.*

Another had this to say:

> *Because of the type of society we live in, which does not even consider creating jobs for the youth, I don't believe there will be a solution to tackling cybercrime anytime soon. If things keep going this way, we'll have no choice but to look for anything to do that will pay us money. It will be difficult to return to our previous state of unemployment once cyber fraud has given us what we want*

Based on the respondent's findings, it can be concluded that unemployment tends to push people towards crime in order to survive financially, and that unemployment also tends to exacerbate among the unemployed, which is linked to criminal conduct. As a result, unemployment is one of several probable influences on students who engage in cyber fraud.

4.2.3 Peer influence

It was also found that majority of the respondents also engage in fraudulent acts in one way or the other due to the desire to belong to the class of their peers. The respondents recounted that those who engage in this fraudulent mostly make a lot of money and they usually exude opulent lifestyles. Hence, in order for them to also be regarded as part of the group, they also joined in the act. They further mentioned that lifestyle of their friends who engage in cyber fraud also looked appealing to them and hence, it took little efforts to lure them into engaging in it.

Respondent 5 affirmed that:

> *"There is this life that they live that when you see, you feel tempted to also have that. You know, they are able to buy anything they want and they get the latest products like phone, shoes, dresses and the likes. When I see things like that too, sometimes I used to feel that I am not part of them because I wasn't having those things they had. So I easily joined so that I can be living like them too and feel comfortable when with them".*

Respondent 3 also mentioned that:

> *"It was not difficult for me to start engaging in this because I used to be very hungry because I had no money and I was almost all the time depending on my friends who do this to feed myself. So when they presented the opportunity for me to join, I just joined. I saw it as opportunity to also enjoy money and be a part of the group. The thing is that sometimes I feel uncomfortable walking with them and asking them for stuff when I am in need. I started a part-time job so I can earn something but still wasn't enough for me and I couldn't even live like them like the way I desired. Since I joined them, I just feel like one of them and flow better with them".*

Respondent 1 also asserted that:

> *"When I wasn't doing this, I used to see some of my friends and the way they were living and sincerely I wished I could have the things they were having. When you walk with them, you will see the difference because you don't wear the dress they wear, you don't hold the phone they hold and you can't go places they can afford to go. I was influenced greatly by the way my friends were living and how they helped me when I had nothing".*

4.3: What Are The Perspective Of The Youth About Curbing Cyber Fraud Among The Youth In Ghana?

It was thought that considering the perspective of the youth in curbing cyber fraud would provide important information on the settings that can help shape or bring to a minimal fraudulent attitudes and mentality about making a living as a youth. In general, the data revealed that all of the respondents said if there was enough available jobs, cyber fraud awareness, opportunities for youth entrepreneurship, a support system which gives the youth an easy access to business partners and Capital Loans among others. Respondent's decision of engaging in cyber fraud could have been thought of. These would not have been a problem, if as a youth in Ghana, there was mechanism, which could easily get us employed or expose us to opportunities to be able to vent for our (youth) individual needs.

4.3.1 Investment in youth technological skills and Job Creation.

Some of the respondents indicated that, they are highly skilled in technology in its usage. They asserted that government will need to pay attention to helping the youth advance their technological ideas and skills so they can be very useful in the formal sector.

In one of the interviews conducted, a respondent claimed:

> *My brother and I are both involved in cyber fraud. Because we are adults and not staying together, he usually calls me once he has a job for me. And because he is a tech savvy he could possesses my BVN (Biometric Verification Number). He will give me the transaction ID and I will go pick up the money for him, but if he wants me to do something that requires my presence, I will have to travel to his location. Because what we are doing is not legal, I am doing it (cyber fraud) with my brother. As a result, I am unable to do so with an outsider.*
>
> *I believe that if I do it with my own blood, I will still be protected. And all of this started after he was laid off from his work, due to initiative of the government to collapse non performing banks in the country. My brother was my support system, he was the one helping me with my financial challenges, so after months of not securing a new job, his friend introduced him to fraud and to be frank it has really helped us a lot to be frank. If there was, ready available jobs he could have landed himself a new job, after his dismissal without having the thought of using his technological ideas to dupe people off to make a living.*

In the words of another respondent:

> *Because my father was unable to pay my school tuition and I had to hustle on my own. I was working as a shop attendants to fetch myself*

> *some money. I was used and was not getting paid consistently so could not hit my savings target. My Godmother, who was also my school mother in the senior high school, introduced me to internet fraudsters (Chairmen). Since then I got addicted to the game and my life has never been the same financially. Because any transaction they use my ID card, picture or phone number to do on their behalf, I get paid very well. An amount which could not be made even if I was doing a monthly sales Job was now earned on daily basis depending on how frequent work comes.*
>
> *So I took it as an opportunity to make enough money with these perpetrators (chairmen) and use my earnings as my capital to start my online business. Because as young as I am, if I should go to the bank to access loan without a collateral for my business, I will not get. In other words the government should make it easy for the youth to acquire capital to self-finance their education or pre business ideas into reality. Sure, it might not solve the problem completely, but at least the smart business minded ones in it might draw out to build their dreams.*

A respondent had this to say:

> *My best friend who is also technologically inclined as I am introduced me to it (cyber fraud) and seeing how they (other people involved in cyber fraud) do it and get money,I also started because nobody wants to live without having money. Looking at them, and seeing the way they are doing stuffs, and at the end they usually come up with money, there is no way one would not have interest in it. So in my own view, I believe if the government really want to minimize or eradicate fraud in our society, then they should be very serious and invest in youth technological advancement programs. So the youths who are really tech inclined like myself will get employment space to utilize my skills in the corporate world.*

Another respondent asserted that:

> *I am amongst the millions of youth in Ghana who are highly skilled with technological stuff but we are not being useful. The government needs to pay attention to the youth in technology and upgrade our skills so that it can employ us in the various governmental organisations. If this is taken seriously, the issue of fraud will drastically stop because many youth are into this because there are no jobs for them. It is not something that is good, I mean, the cyber fraud but it is the situation that is causing this".*

4.3.2 Public education.

Some of the respondents conceded that there is the need for public education for people to become alert of the fraudulent tricks being played by these fraudsters to extort certain vital information and money from their victims.

A respondent mentioned:

> *It is something I have always done (cyber fraud). I was successful the first time I attempted it. As a result, I was inspired to do more. In fact, I have never learned anything from a bunch of individuals. I learned it from a specific person, who happens to be a friend of mine. I normally talk to him about any issues I am having with my scheme. I usually ask him for information whenever I need it. So in my view I think there should be massive education on how these perpetrators' operate, to caution the public on awareness never to let anyone loose him or herself to a victim of fraudulent activities like, mobile number hacking, whatsapp hacking among many others. So that if there is no easy access or means of hacking anyone, it will definitely discourage you from perusing your fraudulent activities goals.*

Another respondent indicated that:

> *There should be some education made to the publics (both nationals and foreigners) about how fraudsters steal from some of them on the internet. If this happens, it will affect the work we do but I also feel guilty about we do. Sometimes, when I am alone I begin to feel bad when I remember how I am stealing from innocent people from the internet. Although, I am calling that there should be massive education about the mode of operation of fraudsters, government should also try and create jobs for us so that we can stop these fraudulent activities".*

According to the above submissions, university student's perspective of the youth about curbing cyber fraud is for the government to make the system favorable for the youth's voice to be heard in any political administration and for public education to be intensive on the mode of operation of fraudsters.

The conclusion that can be drawn from this study is that family and associates of university students initiated them into cyber fraud perpetration. This research implies that university students are more likely to be open to cyber fraud if their siblings or friends have been involved in it purposely to seek financial freedom. This finding is also consistent with Ige's (2008) findings, which found that secondary school pupils in the Nigerian states of Oyo and Ondo were being introduced into Cyber fraud by their friends at universities, polytechnics, and colleges of education. It also supports a key claim of social learning theory, namely: deviant behavior, which is more likely to occur when a person associated themselves with people who engage in an unapproved or deviant behavior rather than persons who do not.

Furthermore, this finding is consistent with Miller and Morris's (2014) findings, which found that relationships with delinquent peers who had a history of cyberbullying has a significant impact on people's proclivity for such new deviant behavior.

4.3.3 Punitive measures.

The respondents also recounted that, ensuring that perpetrators of this act are punished severely when caught, is another way to curb the situation. Though, they conceded severe punishment as a good measure, majority of them asserted that the best way to go is to ensure that more jobs are created for the youth in order to get them disinterested in the fraudulent act.

One respondent mentioned that:

> *"Another thing that can be done is by punishing those who engage in it when they are caught. Many at times, the police and the security agencies have even become friends with those who engage in it. They normally send these police men huge sums of money into their account when they "cash out". If this continues, those engaged in it will not be scared of the authorities and they won't stop any moment soon. I have some friends who have made a lot of friends with the police men. Even for some of them, when they have issues they just call their "police friends" and they come and rescue them all because of money. If perpetrators are not seriously punished dieerr, then this thing will*

> *continue for a very long time. The most important thing to do is to create more jobs for us".*

Another respondents also affirmed that:

> *"If people go wrong and caught and they are not punished, what do you expect? They will continue to do that wrong thing because after all, they know they won't be punished for the wrongdoing. So for me, the security agencies should be proactive and be serious about dealing with things like that. For some of us, maybe when we see others being punished for this, maybe we can stop. I'm not even motivated to stop because I have some of my friends who have connections and so even if I get into trouble I will easily escape".*

Again, the responses above indicate that the security agencies seem not to be firm in the fight against cyber fraud. It suggests that some workers in the security agencies are accomplices in the act as they shield some of cyber criminals that get caught.

Another respondent also added that:

> *"Though I am also of the view that criminals should be punished very well when caught to deter others, I think that is not the sure way to end this. There needs to be measures put in place to ensure that the youth get work to do. By this, there will be regular income for them and they will not even have that motivation to engage in fraud. For me, I feel bad usually when I sit down and think about I do. I feel bad sometimes because it is against my religion. I am a Muslim and Allah does not encourage us to steal. You know….this is stealing and it's bad. Let's tackle the issue from the bottom. There should be jobs because many youth are forced into this due to certain circumstances".*

4.3.3.1 Chapter Summary

This chapter presented a rich and detailed analysis of the findings from the collected data. The study sought to examine cyber fraud among the youth in Ghana using some student in a private university. The study found that Participants' involvement in cyber fraud was accounted for by a variety of push and pull. Also, only a few of the participants engage in cyber fraud because they want to have fun and be entertained, While the majority of participants nearly 80% of them engage in cyber fraud as a result of peer pressure and financial necessity. This finding confirms Cohen and Felson (1979) assertion that, emphasizes that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian and also the space transition theory that proposes that people who have restrained criminal activity (in physical space) are more likely to do so in cyberspace than they would in physical space due to their status and position.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

This chapter provides the summary of the findings. It also presents recommendations and possible suggestions for future research.

5.1 Summary

Three important findings from the research can be summarized in the above discussion. First, this study revealed that cyber fraud is on the rise in Ghana, particularly among university students, which was confirmed by a prior study by IC3 (2010); Oduro- Frimpong (2011).

Some interviewees, indicated that Ghana is now the 'headquarters' of West African cyber fraudsters. Others saw it as an occupation for some of the country's youth who were unemployed. According to the data acquired, the most common type of Cyber fraud performed by practically all fraudsters is the confidence/romance scam. The next sort of cyber fraud used by most students was gold format and agriculture/construction format.

However, it is debatable why the majority of students, particularly university graduates, in the country choose to practice cyber fraud as a source of income. The grounds for such engagement were discovered to be both intrinsic and external. The majority of the students who engaged in the deception attested to their involvement and linked it to a desire to become financially stable in life. Poverty as a result of unemployment was also noted as a contributing reason to the participant's inactions. Extrinsic variables in the practice of Cyber fraud in universities included peer pressure and a lack of parental care. As a result, the Routine activity theory and the Space Transition theory are supported.

5.2 Limitation of the study

The study's data collection was limited due to the small number of participants. Aside from the academic cycle, the study was based on the opinions of participants, and their data is not permitted to be shared with third parties for ethical reasons.

The investigation was limited once again by the need to meet the research deadlines. To be able to accurately describe how Cyber Fraud was practiced, the researcher had to record and transcribe the interview sessions, which affected the time element or frame given for data gathering. Furthermore, studying how the act was performed throughout time could yield variable results because the type of act impacted the topic that would be explored, casting doubt on the study's thorough character.

However, throughout the course of ninety days (January 10, 2022 - March 31, 2022), the researcher obtained sufficient data from four different types of cyber fraud in Ghana, providing useful information on how the act was carried out and the instruments utilized in carrying it out. The research sample was limited to students.

5.3 Recommendations

As a means of resolving the issue of cyber fraud, the following recommendations are suggested:

Government needs to invest in youth technological skills and create more jobs for the youth. The government needs to institute measures that harness the skills and talents of youth in I.T by promoting I.C.T education from the lowest level to the highest level of education. Not only should the education of I.C.T be promoted and prioritized, but there should also be more jobs created to motivate the youth to acquire education and be useful to themselves, their families, communities and the nation at large.

Public education also needs to be intensified by the communication ministries and its agencies about key cyber issues for victims and prospective victims of cyber fraud not to suffer the huge ramification of falling prey to such acts. Intensive public education also need to be carried out nationwide about the law regarding cyber security and cyber fraud and the legal implications for those who engage in cyber fraud activities.

The punitive measures established in the constitution for those who perpetrate cyber fraud need to be fully implemented and not negotiated for personal interests and self-aggrandizement. There is the need for security agencies and their agents not to be influenced by money or gifts in the discharge of their duties. Also, the ministry of communications can also put in place measures to greatly reward security agents that interdict perpetrators of cyber fraud activities whilst also severely punish those that shield perpetrators of the fraudulent acts.

5.4 Suggestions for future research

The growth of Cyber fraudsters has increased the use of technology in criminal investigations. While there are several tools and methods that investigators might utilize to aid in their work, none of these technologies can do all the tasks necessary by themselves. It is therefore crucial to get knowledgeable about various technologies, how they operate, and the kinds of information they might provide to investigators in resolving cyber fraud situations. Therefore, the researcher suggests that future research on cyber fraud should focus on the tools that cyber fraudsters use to carry out their actions, as well as how they manage to maintain their affluent lifestyles without drawing the attention of any security agencies or raising any red flags. Finally, they can research how cyber fraudsters manage to withdraw sizable sums of money from banks covertly.

REFERENCES

Abbey, N. R., (2009, June 03). Internet fraud to modern day sakawa. The untold synonymize. *Modern Ghana*. www. modernghana.com

Abugri, S. G., (2014, April 28). Ghana: Internet criminals cash in on e-waste dumping. *Action fraud*. www.scamsurvivors.com

Adeniran, I.A. (2008). The Internet and Emergence of Yahooboys sub-Culture in Nigeria. *International Journal of Cyber Criminology*, *2*(2), 368. https://www.cybercrimejournal.com/adebusuyiijccdec2008.pdf.

Aderinto, A. A., & Ojedokun, U. A, (2017). Cyber underground economy in Nigeria. *Cyber criminology and technology assisted crime control: A reader (pp. 219-226)*. Zaria, Nigeria: Ahmadu Bello University Press. www.semanticscholar.org

Ahmed, A. (2007). Open access towards bridging the digital divide–policies and strategies for developing countries. *Information Technology for Development*, *13*(4), 337–361. https://doi.org/10.1002/itdj.20067.

Amando F. (2015). Internet Fraud Rising In Ghana and Many other West African Countries. *Society of Ghanaian Scammers*. www.gh.usembassy.gov

Annan, J. (2015). Security Alert: Cyber Fraud on Rampage. Centre for Strategic and International Studies. *Modern Ghana*. www. modernghana.com

Armstrong, A. (2011). Sakawa Rumours. *Occult Internet Fraud and Ghanaian Identity*. www.ucl.ac.uk

Asamoah, G. N. & Agyapong, D. (2011). Sakawa in Ghana: what problem? Whose problem?' Able Ghana. *Internet Fraud*. www. police.act.gov.au

Barber, K. (1997). Preliminary notes on audiences in Africa. *Africa*, *67*(3), 347–362. https://doi.org/10.2307/1161179.

Bennett, R. R. (1991). Development and Crime: A Cross-National, Time-Series Analysis of Competing Models. *The Sociological Quarterly*, *32*(3), 343–363. https://doi.org/10.1111/j.1533-8525.1991.tb00163.x.

Draman, A. R., Berdal, M., & Malone, D. M. (2000). Greed and Grievance: Economic Agendas in Civil Wars. *International Journal*, *55*(4), 682. https://doi.org/10.2307/40203523.

Best, S. (2006). Introduction to peace and Conflict Studies in West Africa: A Reader. *Ibadan: Spectrum Books Limited.* Worldcat.org

Boateng, R., Babatope Longe, O., Mbarika, V., Avevor, I. & Isabalija, S. I. (2009). Cyber Crime and Criminality in Ghana: Its Forms and Implications. *Americas Conference on Information Systems*, 507.

https://sci.ui.edu.ng/sites/default/files/Cyber%20Crime%20and%20Criminality%20in%20Ghana.pdf.

Boateng, R., Longe, O.B., Isabalija, R., &Budu, J. (2011). ‘‘Sakawa’’ Cybercrime and criminality in Ghana. *Journal of Information Technology Impact. 2 (11). Pp.85-100.*

Susan W. Brenner, & Leo L. Clarke. (2005). Distributed Security: A New Model of Law Enforcement. *Social Science Research Network*. https://papers.ssrn.com/sol3/delivery.cfm/ssrn_id845085_code546543.pdf?abstractid=845085.

Brenner, S. W. (2006). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law & Criminology*, *97*(2), 379–476. https://dialnet.unirioja.es/servlet/articu.

Broadhurst, R., & Chou, R., (2009). Cybercrime and online safety in Cyberspace. *International handbook of criminology.* http://dx.doi.org/10.4324/9780203864708.ch16.

Burell J., (2008). Research Article Problematic Empowerment: West African Internet Scams as Strategic Misrepresentation. (2007). *Information Technology and Africa Development*, *4 (4), 15-30*.

Button, M., Lewis C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: literature review. (2008). *National Fraud Authority*. https://puredev.port.ac.uk/en/publications/fraud-typologies-and-the-victims-of-fraud-literature-review.

Button, M., Lewis, C., &Tapley, J. (2009). Support for the victims of fraud: an assessment of the current infrastructure in England and Wales. (2008b). National Fraud Authority. *Research Portal.* https://researchportal.port.ac.uk/portal/files/1926164/support-for-victims-of-fraud.pdf.

Button, M., Tapley, J., & Lewis, C. (2013). The ‘fraud justice network’ and the infra-structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice*, *13*(1), 37-61.

Chapple, C. L., & Hope, T. L. (2003). An Analysis of the Self-Control and Criminal Versatility of Gang and Dating Violence Offenders. *Violence and Victims*, *18*(6), 671–690. https://doi.org/10.1891/vivi.2003.18.6.671.

Chon, S. (2013). Routine Activity Theory and Cybercrime: What about Offender Resources? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2379201.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589.

Collier, P. (2000). Paul Collier. (1999). Economic Causes of Civil Conflict and their Implications for Policy. *Leashing the Dogs of War*. http://stefanwolff.com/reset/ethnic-conflict-theories/downloads/collier.pdf.

Commission for Human Security (CHS). (2003). Human Security Now. *United Nation digital library*. www.digitallibrary.un.org

Coomson, J. (2006). Cybercrimes in Ghana. Ghanaian Chronicle. *All Africa*. www.allafrica.com

Croall, H. (2007). Victims of White-Collar and Corporate Crime. *Victims, Crime and Society*, 78–108. https://doi.org/10.4135/9781446212202.n4.

Danofsky, S. (2005). Open access for Africa: challenges, recommendations and examples. *The United Nations Information and Communication Technologies Task Force*. https://agris.fao.org/agris-search/search.do?recordID=XF2006409780.

Danquah, P., &Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. *African Journal of Computing & ICTs, 4(2), 37-48.* www.citeseerx.ist.psu.edu

Deevy, M., Lucich, S., & Beals, M. (2012). Scams, schemes & swindles: A review of consumer financial fraud research. *Financial fraud research center*.www.longevity.stanford.edu

Doig, A. (2008). Fraud Cullompton: Willa. *Criminology and criminal justice*. www.journals.sagepub.com

Electronic Communication Act 775 (2008). *Electronic Transaction Act*. www.moc.gov.gh

Eliasson J., (2011). Peace Development and Human Right. *The indispensable Connection*. Sweden: Uppsala University. www.daghammarskjold.se

Essel, I. (2009, August 12). National Youth Policy to solve 'sakawa'. *My Joy Online*. www.myj oyonline.com

Faleti, S. A. (2006). *Theories of social conflict*. In G.S Best (Ed.), Introduction for peace and conflict studies in West Africa. Ibadan: Spectrum Books Ltd. pp.35-60. Worldcat.org

Federal Bureau of Investigations, (2011). Financial crimes report 2010-2011. *U.S. Department of Justice* .www.fbi.gov

Felson, M. (1998). Crime and Everyday Life. *Criminology and Criminal Justice Series*. http://ci.nii.ac.jp/ncid/BA58946329.

Felson, M. (1993). Crime and Everyday Life: Insights and Implications for Society. *SAGE Publications, Inc*. https://ci.nii.ac.jp/ncid/BA21918483.

Cohen, L. E., & Felson, M. (1979b). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589.

Identity Theft: Trends and Issues. (2010). *Congressional Research Service*. http://research.policyarchive.org/18922.pdf.

Fraenkel, J. (2022). *How to Design and Evaluate Research in Education* (International). McGraw-Hill Education.

Francis, D. J. (2006). *Uniting Africa: Building Regional Peace and Security Systems* (1st ed.). Routledge.

Frimpong- Oduro Joseph (2011). 'Sakawa': On Occultic Rituals and Cyberfraud in Gh anaian Popular Cinema. *Cambridge University Press 57(2).pp.131-147*.www.jsto r.org

Galtung J. (1969). Violence and Peace Research. *Journal of Peace Research, Sage Pu blications, Inc. 6(3) 167-191*.www.jstor.org.

Galtung, J. (1990). Cultural Violence. *Journal of Peace Research*, *27*(3), 291–305. https://doi.org/10.1177/002234339002700300 5.

Galtung. J. (1996). Peace by Peaceful Means: Peace and Conflict, Development and Civilization. *Development and Civilisation. PRIO's Publications Publications*. https://doi.org/10.4135/9781446221631.

Gee, J., Button, M. & Brooks, G. (2009). The Financial Cost of Healthcare Fraud 2015: What Data from Around the World Shows. (2009). *Mark Button and Graham Brooks.* https://researchportal.port.ac.uk/portal/files/17778625/The_Financial_Cost_of_Healthcare_Fraud_Report_2014_11.3.14a.pdf.

Ghana Business News (2010). Ghana, Nigeria cited among top 10 countries in global cybercrime ranking. *Ghana business news*. www.ghanabusinessnews.com

Ghosh, A., (2013). Seclayer: A plugging to prevent phishing attacks. *The IUP Journal of Information Technology, Vol. 9, (4).pp. 52-64.* www.papers.ssrn.com

Ginsburg, F. (1994). Embedded Aesthetics: Creating a Discursive Space for Indigenous Media. *Cultural Anthropology*, *9*(3), 365-382. https://doi.org/10.1525/can.1994.9.3.02a00080.

Global Internet Report (2015). Mobile Evolution and Development of the internet. *Global Internet report.* www.future.internetsociety.org

Guerra, P. (2009). How economics and information security affects cybercrime and what it means in the context of a global recession. *Turbo Talk.* www.blackhat.com

Catherine Hakim. (1999). Research design : successful designs for social and economic research. *Routledge*. https://ci.nii.ac.jp/ncid/BA47065240.

Hawdon, J. (1999). Daily routines and crime using routine activities as measures of hirschi's involvement. *Youth society*.www.doi.org

Hughes, R. B. (2009). NATO and cyber defense: mission accomplished? *Nato Otan.* www.csl.armywarcollege.edu

International Telecommunications Union (2008). Africa, ICT Indicators 2007. *ITU World Telecommunication/ICT Indicators Database.* www.itu.int

International Telecommunications Union (2009). ICT Statistics Database. *ITU World Telecommunication/ICT Indicators Database.* www.itu.int

International Telecommunications Union (2007). ICT Statistics Database. *ITU World Telecommunication/ICT Indicators Database.* www.itu.int

International World Statistics (2011).Internet World Stats - Usage and Population Statistics. *ITU World Telecommunication/ICT Indicators Database.* www.itu.int

Internet Complaint Centre (2008). IC3 2008 Annual Report on Internet Crime. *Federal Bureau of Investigation.*www.ic3.gov

Internet Crime Complaint Centre (2008). Internet Crime Report Internet Crime. *Federal Bureau of Investigation.*www.ic3.gov

Internet Crime Compliant Centre (IC3). (2006). Internet Crime Report. U.S. Department of Justice. *Federal Bureau of Investigation.*www.ic3.gov

Internet Crime Compliant Centre (IC3). (2010). Internet Crime Report. U.S. Department of Justice. *Federal Bureau of Investigation.*www.ic3.gov

Internet Fraud Complaint Centre (IFCC). (2001). Internet Fraud Report. *National White Collar Crime Center and the Federal Bureau of Investigation.*www.ic3.gov

Internet Fraud Watch (2002). Internet Fraud Statistics: 2002 Top 10 Frauds. *International Journal of Accounting and Management.* www.researchgate.net

Jadquith S. M. (1981). Adolescent marijuana and alcohol use: in empirical test of differential association theory, criminology. *Criminology 19*(2).

Karuppannan Jaishankar. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, *1*, 7–9. https://doi.org/10.5281/zenodo.18792.

Jegede A. E., (2014). *Cyber fraud, Global trade and youth crime burden: Nigeria Experience.* Prentice Hall. www.academia.edu

Jeremy H. (2017). Introduction to Study Design. jeremy.howick@phc.ox.ac.uk)

Kerr J., Owen R., Nichollas M. C., & Button M. (2013). Research on Sentencing Internet Online Fraud offences. *School of Criminal and Criminal Justice*. researchportal.port.ac.uk

Kruse, W.G. & Heiser, J.G. (2002). Computer Forensics: Incident Response Essentials. (2001). *Journal of Information Security*. https://ci.nii.ac.jp/ncid/BA56079235.

Kunz, M., & Wilson, P. (2004). Computer crime and computer fraud. *Report Submitted to the Montgomery County Criminal Justice Coordinating Commission*.

Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22–31. https://doi.org/10.1145/1629607.1629613.

Levi, M. (2001).White Collar Crime, Consumers and Victimization. *Hal Open Science.51 (1), pp.127-146.*www.hal.archives-ouvertes.fr

Levi, M. (2008). Organised frauds and organizing frauds: Unpacking the research on networks and organisation. *Criminology and Criminal Justice, 8*(4), 389–419. www.journals.sagepub.com

Lundeberg, M. A., & Scheurman, G. (1997). Looking twice means seeing more: Developing pedagogical knowledge through case analysis. *Teaching and Teacher Education*, *13*(8), 783–797. https://doi.org/10.1016/s0742-051x(97)00020-6.

Lynch, J. P. (1987). Routine activity and victimization at work. *Journal of Quantitative Criminology*, *3*(4), 283–300. https://doi.org/10.1007/bf01066832.

Marsh J, C. (2004). Key Concepts for Understanding Curriculum. (2009). *Routledge*. https://doi.org/10.4324/9780203870457.

Melzer, M. (2011). Cyber-warfare & international laws. *UNIDIR International law*. www.unidir.org

Nalla M, (2014). Theorising Cybercrime: Applying routine Activity Theory. *Micah-Sage* .www.academia.edu

Ninson.C, (2017). Internet fraud and its socio-economic implications for peace and development of Agona Swedru (Ghana). (2017). *Sam Jona Library*. https://ir.ucc.edu.gh/xmlui/handle/123456789/3416.

Bolden. National Fraud Authority (2010). Annual Fraud Indicator. *National Fraud Authority*. www.attorneygeneral.gov.uk

National Fraud Authority (2010). Fraud typologies and Victims of Fraud. *National Fraud Authority*.www.gov.uk

National Fraud Authority (2011). Annual Fraud Indicator *National Fraud Authority*.www.gov.uk

National White Collar Crime Centre (2008). Reported Dollar Loss From Internet Crime Reaches All Time High . *National Fraud Authority*.www.ic3.gov

NATO (2004) 'NATO policy on combating trafficking in human beings'.Nato *Research Centre.* www.nato.int

Neuman, W. L. (2000). *A guide to using qualitative research methodology*. Boston. Allyn and Bacon Publishing. www.Scirp.org.

Neuman, W.L. & Kreuger, L. W. (2002). Social work research methods : qualitative and quantitative approaches. *Allyn and Bacon*. http://ci.nii.ac.jp/ncid/BA65616583.

Graeme R. Newman, & Megan M. McNally. (2005a). Identity Theft Literature Review. *United States. Department of Justice*. https://www.hsdl.org/?abstract&did=456009.

Obosu M., (2009). "Sakawa", Genesis and Effect. *Ghana Web News*.www.ghanaweb.com

Oduro-Frimpong, J. (2011). 'Sakawa' on occultic rituals and cyberfraud in Ghanaian popular cinema. *Southern Illinois, University Carbondale*. www.easaonline.org

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010b). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903.

Pret. A., (2009), Internet fraud and its effect on the economy: A Case Study of Banking Institutions in Nigeria. *Journal of Internet Banking and Commerce pp.15 (1), 35-47*. www.citeseerx.ist.psu.edu

Rantala R.R., (2008). Cybercrime against businesses. *United State Department of Justice Bureau of Justice Statistics.* USA. bjs.ojp.gov.

Susan, W., Brenner, S. W. & Leo, L. & Clarke, M. (2005). Distributed Security: A New Model of Law Enforcement. *Social Science Research Network*. https://papers.ssrn.com/sol3/delivery.cfm/ssrn_id845085_code546543.pdf?abstractid=845085.