University of Education,Winneba http://ir.uew.edu.gh

UNIVERSITY OF EDUCATION, WINNEBA

COLLEGE OF TECHNOLOGY EDUCATION – KUMASI CAMPUS

CYBERCRIME IN BANKS, STUDY IN KUMASI METROPOLIS

BY

BAFFOUR OSEI BONSU

SEPTEMBER, 2022

University of Education,Winneba http://ir.uew.edu.gh

UNIVERSITY OF EDUCATION, WINNEBA

COLLEGE OF TECHNOLOGY EDUCATION – KUMASI CAMPUS

CYBERCRIME IN BANKS, STUDY IN KUMASI METROPOLIS

BY

BAFFOUR OSEI BONSU

(7181000010)

A Dissertation in the Department of Information Technology Education, Faculty of Technical Education, submitted to the School of Graduate Studies in partial fulfilment of the requirements for the award of the degree of Master of Science (Information Technology Education) in the University of Education, Winneba

SEPTEMBER, 2022

University of Education,Winneba http://ir.uew.edu.gh

DECLARATION

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where states otherwise by reference or acknowledgment, the work presented is entirely my own.

Signature: ……. Date: ……

BAFFOUR OSEI BONSU

SUPERVISOR'S DECLARATION

I hereby declare that the preparation of this project was supervised in accordance with the guidelines on supervision of long essays laid down by the University of Education, Winneba.

Signature: ……. Date: ……

DR. SAMUEL ADU GYAMFI

University of Education,Winneba http://ir.uew.edu.gh

ACKNOWLEDGMENTS

Thanks to the Lord of hosts for making everything conceivable and with whom this proposal has perceived the light of the day. I am most grateful to Dr. Samuel Adu Gyamfi whose commitment, constructive criticisms, and suggestions have fine-tuned the outcome of the research.

Furthermore, appreciation goes to the personnel of the Ghana Police Service for the insightful information shared with me. Solomon Idun has greatly been a helper and assisted me when I am not around.

University of Education,Winneba http://ir.uew.edu.gh

DEDICATION

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents, Francis Osei Bonsu and Regina Duodu whose words of encouragement and push for tenacity ring in my ears. Also, my gratitude goes to my grandmum Akosua Aberafi. My brother Minkah and my sisters Ntiriwaa, Serwaa, and Adoma have never left my side and are very special. I also dedicate this dissertation to my many friends and church family who have supported me throughout the process. I will always appreciate all they have done, especially Rev. Eric Akwasi Mfum. I dedicate this work and give special thanks to my best friend Ankrah Brian for being there for me throughout the entire master's program.

University of Education,Winneba http://ir.uew.edu.gh

ABSTRACT

Cybercrime is an issue that has attracted the attention of financial institutions, credit bureaus, state legislators, and most certainly law enforcement agents. Cybercrime is presently the most-announced kind of crime by financial institutions, and as suppliers of the national framework through their financial administrations, the manners by which these organizations react to and comprehend dangers is of specific significance to a country's security and strength. The goal of this study was to evaluate bank cybercrime. However, the specific goals were to determine facets of cybercrime, investigate major threats that banks face in today's cybercrime, and determine ways to mitigate cybercrime in banks. It was found that operating a bank in this technological age is a challenge and risky because of cybercrime. The investigation reveals that Extortions, disclosure of bank secrets, weaknesses in the management of online transactions, and hacking have made banks vulnerable to exploitation. This action has helped cyber fraudsters to perpetuate their treacherous act with ease. Adopting public education on cybercrime and, the right banking measures and building better internet and cybersecurity systems that have the propensity to avert tendencies of fraud. Again, the website of banks must be secured and periodically enhance security mechanisms to avoid vulnerabilities.

University of Education,Winneba http://ir.uew.edu.gh

TABLE OF CONTENTS

Contents **Pages**

University of Education,Winneba http://ir.uew.edu.gh

University of Education,Winneba http://ir.uew.edu.gh

University of Education,Winneba http://ir.uew.edu.gh

LIST OF TABLES

University of Education,Winneba http://ir.uew.edu.gh

LIST OF FIGURES

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Cybercrime is presently the most-announced kind of crime by financial institutions, and as suppliers of the national framework through their financial administrations, the manners by which these organizations react to and comprehend dangers is of specific significance to a country's security and strength (Stickings, 2016). Cybercrime is an issue that has attracted the attention of financial institutions, credit bureaus, state legislators, and most certainly law enforcement agents.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. This study is specifically dealing with cybercrime activities in the banking sector in Ghana with a specific location to be Kumasi. This work shows that the gravity of cybercrime is immense, and it can have disastrous consequences. It can demolish the image, reputation, credibility, and health of the victim and tarnish the image of the financial institution. It can also lead to humungous monetary losses to the banks and financial institutions, and lead to unjust enrichment. It possesses the potential to destroy the online economy and deprive it of any faith and trust from the general public and/or users of the internet. It can open up Pandora's box for the criminals, providing them an invisibility cloak, and

University of Education,Winneba http://ir.uew.edu.gh

cause disturbing problems of law and order. But the laws dealing with banking transactions and the laws dealing with crimes are silent on the issues of cybercrime in banking in Ghana.

The job of ICT in a rising economy like Ghana has been broadly perceived at different levels. The acknowledgment is reflected in activities, for example, the advancement and organization of national ICT foundations, and institutional and administrative systems for dealing with the part. Furthermore, the advancement by the utilization of ICT in all divisions of the economy, actualizing e-administration in government establishments, the development of the National Server farm, the Workstation per tyke strategy show that Ghanaians have grasped the learning-based society and Ghana grasping the paperless framework in our harbor and other government segments. The commitment of ICT to the Gross Domestic product expanded from 2.3 percent in 2009 to 10.5 percent in 2011 also, and the industry made 3,500 additional jobs in 2011 contrasted with 3,050 in 2010 (National Development Planning Commission, 2012).

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. From the perspective of ICT for development, it is not misplaced to say that cybercrime portends some dangers and has the potential to stall the developmental contributions accruable from a well-harnessed ICT adoption, diffusion, and usage in Sub-Saharan Africa (Salifu, 2008).

1.2 Statement of the Problem

The web has turned into a twofold-edged sword giving chances to people and associations and carrying with it an expanded data security hazard (Magele, 2005).

University of Education,Winneba http://ir.uew.edu.gh

In Ghana, the rapid adoption of information technology (IT) in daily life (particularly banking) has resulted in a slew of issues. In any case, the trend has recently shifted. This is because, in this wired world, the law enforcement community faces difficulty as information technology advances. It may be simple to ask a computer wizard to upgrade one's computers or to report computer crimes, but combatting this crime and obtaining effective convictions remains a difficult issue for current legal regimes around the world. Countries are relying on new digital techniques to handle practically every element of daily life, from identity cards to credit cards to health data, as well as the protection and defense of their borders, more and more every day. Ghana Web (2013), disclosed that Ghana has been ranked seventh in the world and second in Africa in terms of cyber fraud as of that period is alarming. In the quest to become rich instantly amidst economic hardship and high unemployment rate, a large percentage of the youth and young people are involved in different facets of crimes, most especially, cybercrime. The internet, for example, makes it easier for criminals to work across national borders. Credit card transactions from the country have been blocked by several companies in the Western world as a result of cybercrime. To support this notion, Kwablah (2009), the study disclosed that Ghana was the second most frequently blocked area by commercial establishments based on US electronic commerce because shops are suspicious about bogus demands from online con artists. The difficulties faced by Ghanaian entrepreneurs and businesswomen stem from such severe blows to our credibility.

Civil society, NGOs, and opinion leaders have raised their alarm about the rise in cybercrime in the country. The surge of cybercrime in Ghana had caused huge losses to individuals, organizations, and the government as a whole. This has prompted more media coverage, with headlines such as *"Cybersecurity Fund to be Introduced in 2019 Budget" and "Cybersecurity*

University of Education,Winneba http://ir.uew.edu.gh

Fund to be Introduced in 2020 Budget" (National Cyber Security Centre, 2018) "UGBS partners with a cybersecurity company to educate students to combat threats of cyber-fraud (Graphic Online, 2017)", "Legislation on cybersecurity will address weaknesses in our cybercrime laws (National Cyber Security Centre, 2018)", "Parliamentary Select Committee on Communications to train on cybersecurity (Graphic Online, 2019)", "Man, 38, arrested for defrauding banks (Graphic Online, 2019)", "Man, 38, arrested for defrauding banks (Graphic Online, 2019)".

There is no denying that cybercrime is on the rise and has a high index with the above tag reportage.

Be that as it may, the greater part of these cybercrime cases is frequently not reported and the nation does not have an adequate functioning arrangement to ascertain such misfortunes, especially in the banking sector. Individuals and organizations had lost a huge sum of money and assets through cybercrime.

Data from the Criminal Investigation Department (CID) office's Cybercrime Unit shows that Ghana lost over US$25.8 million in 2016, with US$8.4 million in the form of corporate compromises. Gauges further demonstrate that as of August 2018, Ghana had lost US$97 million because of Cybercrime. This is an indication of increasing cybercrime incidence (National Cyber Security Centre, 2018).

Some victims have their bank accounts emptied and others have their asserts sold without their genuine consent. As a result, this study seeks to bring to bear the dynamics of cybercrime in the financial institutions of Ghana.

University of Education,Winneba http://ir.uew.edu.gh

1.3 Study Objectives

The goal of this study was to look into the dynamics of cybercrime in Ghana, with a focus on banking institutions in the Kumasi Metropolitan Area. The study's objectives were to:

1. Outline the facets of cybercrime in Ghana.
2. Identify the threats faced by most banks through cybercrime in Ghana.
3. Explore the strategies to mitigate cybercrime threats in the banking sector of Ghana

1.4 Research Questions

1. What are the facets of cybercrime in Ghana?
2. What are the cybercrime threats faced by most banks in Ghana?
3. How can cybercrime threats be mitigated in the banking sector of Ghana?

1.5 Significance of the Study

The study's findings will aid the government and all stakeholders in developing effective measures for dealing with cybercrime in the banking industry. The proposed solutions can assist the sector in regaining its dampening credentials. Those who perpetrate such crimes to deceive and exploit innocent people and organizations, on the other hand, will be revealed. As a result, this study tried to investigate the components of cybercrime activities in Ghana, with a specific focus on banks in Kumasi city. The knowledge gathered from this study can be added to the academic reservoir of cybercrime and used as a point of reference in the future.

University of Education,Winneba http://ir.uew.edu.gh

1.6 The Scope and Limitations

The study focuses on the use of the Internet to commit crimes in Ghana, as well as the consequences for the country's international image. The focus is mostly on the use of the internet to perpetrate crimes against financial institutions. Unfortunately, because the research was mixed-method and included a significant quantity of in-depth qualitative techniques, the study was unable to contact a substantial number of respondents in Ghanaian locations. The problem was made even more difficult by the constraints of time and money. As a result, the probe was restricted to Kumasi. The city was picked because it receives the most media attention when it comes to cyber fraud. It is often assumed that practically all financial institutions have their headquarters in Accra and provide services to the majority of the country.

1.7 Definition of Key Concepts

To enable an effective interpretation and understanding of the findings of this study, the following key terms/phrases have been operationally defined in the context of the study.

Cyberspace- the realm of computerized interactions and exchanges

Cybercrime- For the study, cybercrime means using ICT as a medium to defraud people which is popularly referred to as "Sakawa" in Ghana.

Cyber fraud – is a crime committed via computer with the intent to corrupt another individual's personal and financial information stored online.

Offender - A person who has committed fraud using the internet or cyberspace as a conduit to seek financial rewards.

Threat – intention to cause damage or hostile action on an information system to exploit

University of Education,Winneba http://ir.uew.edu.gh

1.8 Organization of the Study

There are five chapters in the research. The backdrop of the study, the presentation of the problem, the goals and objectives, the importance of the study, the scope and constraints, and the definition of essential words and organization of the study are all covered in Chapter One. Chapter Two covers the literature review, while Chapter Three delves into research methodologies, including design, study area, sampling strategies, sample size, data collection sources, research tools, data analysis, ethical issues, and challenges, encountered when out on the field. The fourth chapter focuses on data presentation and discussion of the results of the interviews. The fifth chapter provides an overview of the cybercrime concerns in banks, as well as a conclusion and strategy options.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

This chapter examined cybercrime data from a variety of sources, including textbooks, certified online journals, periodicals, dissertations, newspapers, websites, organizational reports, and other pertinent materials. A review of the literature, according to Neuman (2003), is based on the notion that information accumulates and that individuals acquire and develop what others have done.

The evaluation of related research, according to Bryman(2008), provides a review of what has been established, who are the important writers, what are the predominant topics, the questions that are posed, and the appropriate study techniques. With this in mind, the following themes were considered: cybercrime in context, features of cybercrime, aspects of cybercrime in Ghana, banking fraud, the impact of cybercrime in financial institutions, proposed solutions to combat cybercrime in Africa, and cybercrime detection and prevention.

2.2 Theoretical framework

As stated by Grant & Osanloo (2014) "Without a theoretical framework, the structure and vision for a study will be unclear, like a house that cannot be built without a plan. A research plan contains a theoretical framework that allows the thesis study to be solid and structured with an organized flow from one chapter to another ". To start with, it is imperative to comprehend what a 'system' is, inside the setting of research. Consider being for research as a structure that gives "direction for the specialist as study questions are calibrated, techniques for estimating factors are chosen and investigations are arranged".

University of Education,Winneba http://ir.uew.edu.gh

2.3 Overview of Cybercrime

When US officials handed ARPANET to civilian administration under the auspices of the National Science Foundation in 1990, it gave the Internet a tremendous boost. In 1990, researchers at the CERN physics laboratory in Switzerland developed an Internet browser (basically a data-sharing application) (Ling, 2004). Dubbed the "internet" (www), this product was developed along these lines by various software engineers, allowing increasingly complex types of data trade, such as the sharing of pictures as well as the content.

According to Aidoo, Akotoye, and Ayebi-Arthur (2012), cybercrime cases stretch back to the mid-1960s, when the first cybercrime case was reported. Since then, there have been many reports of cybercrime being committed regularly (Kabay, 2008). For financial gain, early criminals frequently utilized illegal access to the media communication framework to undermine long-distance telephone systems by modifying or destroying data. In addition, in the 1980s, applications began with harmful software, such as self-replicating programs that interfere with the PC. From the mid-1990s forward, the illicit use of SMS exploded, resulting in a deluge of unsolicited commercial and fraudulent activity (Rollins & Wyler, 2013).

The absence of a consistent and statutory meaning for the behaviours that constitute cybercrime is a simple difficulty for the research of cybercrime (Yar, 2013). When it comes to defining cybercrime, there are a lot of abstract complications and a lot of different information. It is also referred to by a variety of titles, including computer crime, digital crime, information technology crime, Internet crime, and virtual crime, in addition to the difficulties in defining it. Academics, writers, and law enforcement agencies appear to be content to deploy numerous components that constitute cybercrime rather than define it, and it appears that academics, writers, and law enforcement agencies are content to deploy numerous components that constitute cybercrime

University of Education,Winneba http://ir.uew.edu.gh

rather than define it (Olayemi, 2014). A workshop devoted to criminal problems identified with PC systems was held during the 10th United States Congress on Crime Prevention and Offender Treatment in 2005.

In an attempt to characterize cybercrime, the US Department of Justice lays out a three-part definition: First, crimes in which a computer or computer system is the intended victim. For example, hacking, malware, and a denial-of-service assault. The second is a crime in which a computer is employed as a tool to commit the crime. Third, is a crime in which the use of a computer is an unintentional aspect of the crime's execution but may aid in the creation of evidence. The Council of Europe's Cybercrime Convention (CoE) was established in 2001 to address the jurisdictional difficulties raised by the internet's growth (Weber, 2003). Cybercrime is described as "unlawful conduct in which the computer is either a tool or a target" (Suman, Srivastava, & Pandit, 2014). Computer crimes, Weber (2013) said, "refer to a curious type of crime that began cropping up during the nineties as the use of the internet became commonplace all over the world." Drawing on the above definitions, it is critical to emphasize that cybercrime lacks a consistent and legal definition, and it is committed with the assistance of a computer connected to the internet.

2.4 Facets of cybercrime

The 2013 Annual Report of the Internet Crime Compliance Center (IC3), which was released in 2014, detailed the many types of cybercrime reported by individuals. Internet auction fraud, credit card fraud, phony business openings, identity theft, hacking, phishing, and pharming are

University of Education,Winneba http://ir.uew.edu.gh

all examples of these types of fraud. A part of these crimes are exposed in the following segments:

2.4.1 Credit Card Schemes

Credit card fraud is one of the most serious problems facing businesses in the twenty-first century. This occurs when someone uses another person's credit card for a personal purpose and the appropriate card owner is unaware of it (Schmalleger & Pittaro, 2009).

2.4.2 Identity Theft

When someone steals your personally identifiable information, such as your name, social security number, date of birth, and residential or workplace address, they are committing identity theft (Schmalleger & Pittaro, 2009). Identity thieves employ a number of different strategies. These included everything from specialist methods to social engineering. When someone is face to face, on the phone, or a computer, they use deceitful methods to get someone else to give critical information. Most of the time, the social worker is aware of some facts about the person, which leads the unlucky victim to believe that the person is certifiable.

2.4.3 Cyber Pornography and Obscenity

These are exercises that go beyond the boundaries of decency and tolerance. Sexual photos and films are openly available on the internet, resulting in a multi-billion dollar industry (Edelman, 2009). Although these materials are not prohibited, the internet has aided the growth of a diverse network of strange sexual behaviours (DiMarco, 2003). Individuals can use online venues to find others who share their interests, forming stable networks where people can participate in

University of Education,Winneba http://ir.uew.edu.gh

meetings and then endorse their practices. Prostitute clients, for example, frequently utilize technology to communicate with people who share their interests and to request illicit sexual services (Holt & Blevins, 2007). Sexual harassers and other sex-related offenses have grown commonplace on the internet (Olayemi, 2014).

2.4.4 Phishing and Pharming

Phishing and pharming are two common types of fraud that trick victims into thinking they are on a legitimate website, such as their banks when they're actually on a fake one designed to steal their identity and drain their bank accounts (Adeniran, 2008). Every day, millions of e-mails are exchanged around the world, millions of web pages are visited for information, and millions of individuals transact business on the internet. We make every effort to put our faith in the systems that deliver our e-mail when they're actually on a fraudulent website designed to steal their identity and drain their bank accounts (Adeniran, 2008).

2.4.5 Hacking

Hackers are those who have a strong interest in computers and innovation and utilize their knowledge to gain access to computer systems for malicious or exploitative motives. People consider hacking in its malicious setting as a result of financial and personal harm, even though programmers participate in and construct digital security apparatuses. To tell the truth, malicious hacking is typically associated with the production and dissemination of stolen programming that can automate attacks on computer systems. These projects have the potential to disrupt email activity and, on rare occasions, compromise personal data stored on the computer.

University of Education,Winneba http://ir.uew.edu.gh

2.5 Legal Classification of Cybercrime

The concept of cybercrime has sparked a massive amount of research into the various offenses that come under this umbrella term. Wall's (2001) four setup categories are one of the most often recognized and created systems for understanding cybercrime from a legal standpoint:

1. Hacking, defacement, and associated offenses are examples of cyber-trespass.
2. Stealing, deception, and other forms of cybercrime are examples of this type of cybercrime (cash, and property). This leads to credit card fraud, intellectual property theft, and piracy, among other things.
3. Cyber-pornography is a term used to describe behaviour that violates the laws against obscenity and decency.

2.6 Cybercrime- The Global Trend

In today's learning-based data culture and economy, information and communication technologies have proven to be important tools. As a result, governments and commercial organizations are increasingly relying on internet-connected information systems to perform important regulatory and business functions. The UNODC (2013) Yearly Report predicted that, sooner rather than later, it will be difficult to ignore a computer crime and maybe any violation that does not include an electronic proof. To combat online crime, the International Telecommunications Union determined that the worldwide annual loss due to cybercrime is estimated to be between 375 and 575 billion US dollars. The value range is due to the distinguishing technique used by member nations to calculate losses.

From the mid-1990s forward, the unauthorized use of email exploded, resulting in a deluge of unsolicited commercial and fraudulent activity (AVTEST IT-Security Institute, 2019). (Rollins

University of Education,Winneba http://ir.uew.edu.gh

& Wyler, 2013). In today's environment, the growth of software applications has created a challenging dilemma for information security. Due to large data breaches and phishing assaults that reveal billions of usernames and passwords, a new industry for cybercrime covert non-financial accreditations is emerging. Cybercriminals make money by selling stolen badges based on how many individuals use the same username and password on numerous accounts. Verified account credentials usually come at a higher price since they can be used more quickly to take over different accounts, such as creating phony transactions or cash transfers, or hacking Bitcoin and other digital currencies.

Different factors that contribute to the cost of stolen account credentials, however, include the brand, whether or not there is a registered Visa, and how natural it is to exchange products or administrations. Account ratings can now be sold for anywhere from $ 0.20 to $ 15 USD. 1 Computer equipment, such as Guard MBA, teach thieves how to perform rapid guesses of username and passwords, which are sometimes referred to as credential replay attacks. These devices are inexpensive or free to use. Account acquisition success rates can be as high as 5%, resulting in a significant gain of valuable credentials for hackers to utilize for their purposes. Because legacy devices such as web application firewalls (WAF) are not capable of detecting these automated attacks, it can be difficult to detect them.

2.6.1 Social media platforms

Many cybercriminals use social media, transforming it into what may be the fastest-growing communication medium for cybercriminals. They can reach out to a much larger audience by using social media. The platforms are global, simple to use, and do not have any of the costs

University of Education,Winneba http://ir.uew.edu.gh

associated with running a web forum or hosting a website. Active groups from all over the world use Facebook to distribute compromised financial information (such as PII credit card numbers and authorization codes), cybercrime tutorials, malware, and piracy, as well as withdrawal and muling services. Some hackers even use their own identities to sell stolen credit card information and hacking kits.

Figure 1 below shows the most well-known fraud topics posted and examined.

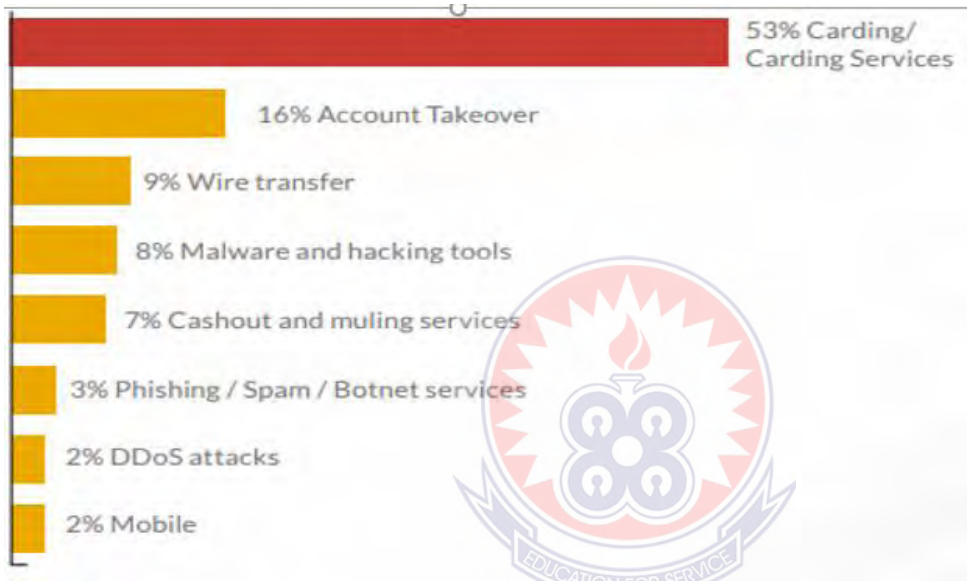


Figure 1: Most Popular Fraud- related posts on Facebook

(*source: Banks & SDI Fraud Report 2020)*

2.6.2 Mobile Fraud

Mobile fraud now outnumbers online fraud. Cell phones are the source of more than 60% of all fraud. It used to be that portable programs were the most fraudulent, but now mobile applications account for 80% of all mobile fraud. As many banks and businesses continue to expand the breadth of services that support their mobile apps, it's a trademark move for cybercriminals. Once a cybercriminal gets complete control over a user's mobile banking app, they can execute tasks like adding new beneficiaries and initiating transfers.

University of Education,Winneba http://ir.uew.edu.gh

RSA (Rivest–Shamir–Adleman) information shows that fraudulent transactions from the mobile channel are more than double the estimate of certified transactions, as it appeared to handle the pattern of this rising crime, the United State of America in the year 2000 set up an Internet Crime Complaint Centre (IC3) which is an organization between the National White Collar Crime Centre (NW3C) and the Federal Bureau of Investigation (FBI) to combat the menace. This security association is to fill in as a conductor for a get-together and sharing data on the internet related to cybercrime. Consistently, the IC3 creates worldwide insights on cybercrime through the data got from the people who have been tricked on the web. Insight investigation is concluded from the report for the yearly examination of cases and to teach unfortunate casualties about the elements of internet scams around the world.

Figure 2 Average Fraud Value vs Transaction value

The circulation of cybercrime cases from 2000 to 2013 is depicted in Figure 2. The IC3 received the most spectacular announced cases in 2009, totaling 336,655 cases from all across the world. In 2013, the IC3 received 262,813 customer complaints, resulting in a total financial loss of $781,841,611, a 48.8% increase over recorded cases of $581,441,110 between 2011 and 2012. The survey also revealed that the United States and the United Kingdom have higher rates of cybercrime victims (0.09 percent), with Nigeria leading the global list of internet fraudsters with

University of Education,Winneba http://ir.uew.edu.gh

an average proportion of 0.97. As a result, the data tries to show that cybercrime can occur regardless of a country's topographical region or financial stability.

Snapshot of Cases captured in IC3 2013 Annual Report

Individuals have been exploited by cybercriminals who have offered rewards, money, business deals, and baited advertisements. According to the IC3 (2013), a subset of these socio-engineering scams arose globally, with the majority of them originating in West Africa. Following that, a discussion of key strategies used by criminals to make messages appear genuine, as detected by IC3, to show the wide range and nature of the scam.

Case 1: A criminal used illegal funds to discredit the Africa Development Bank.

A $5.5 million proposal has been made (Report: 29 April 2013, IC3 Complaint: 11304241115394441)

The Africa Development Bank's (AFB) overarching goal is to promote sustainable economic development and social improvement in its province member states, thereby lowering poverty rates. The AfDB's most important function is to connect Africa's trade with the rest of the world. As a result, the Bank enjoys a high image around the world, but the bad news is that some criminals utilize it to abuse innocent people. This crime method was featured in the IC3 (2013).

Hello, today's praise is for you. I am Mr. Gabriel Compaore, a banker by profession with the African Development Bank (AfDB) in West Africa, where I currently serve as account and exchange manager. I'm sending you this brief letter to request that your organization wire $ 5.5 million to your bank account. Please note that I contacted you since the dead client was a foreigner, and only another foreigner, such as yourself, is eligible to claim the funds. In this light,

University of Education,Winneba http://ir.uew.edu.gh

I decided to contact him with the expectation that I would be safe and secure with his hands since he is involved in a large sum of money worth millions of dollars.

2.7 Cybercrime in Africa

In reality, cybercrime has become a global problem, and no country is immune. In any case, to understand why cyber criminality in Africa differs from other parts of the world, one must first understand the state of data security in this region, which is influenced by factors such as the growth of the user base, a lack of security awareness, a lack of law enforcement training, insufficient regulations, and weak border control. According to the IC3 annual study from 2012, Africa is the third most vulnerable continent to cyber fraud. Nigeria was ranked as Africa's most internet-fraudulent country. Egypt, South Africa, Kenya, Ghana, Zambia, and Cameroon were among the top African countries for cybercrime.

The African Cyberthreat Assessment Report 2021 will assist African governments in identifying the most serious threats and developing a coordinated regional response to cybercrime.

Digital transformation

Cybercrime affects all countries, but African countries are particularly vulnerable because of their inadequate networks and security.

While Africa has an estimated 500 million Internet users, this only accounts for 38% of the population, indicating significant room for expansion. Africa has the world's fastest-growing telephone and Internet networks, as well as the most widespread adoption of mobile banking services.

University of Education,Winneba http://ir.uew.edu.gh

As a result of this digital demand, as well as a lack of cybersecurity policies and standards, online services are at risk. It is vital to put in place a solid cybersecurity framework as African countries attempt to integrate digital infrastructure into all sectors of society, including government, finance, business, and critical infrastructure.

2.7.1 The main cyberthreats in Africa

Based on input from INTERPOL member countries and data from business sector partners, the INTERPOL report outlines the most prominent dangers in Africa.

The following are the top five threats:

Scams on the internet: consumers are tricked into providing personal or financial information by receiving phony emails or text messages pretending to be from a trustworthy source.

Victims are duped into giving sexually compromising images, which are then used to blackmail them.

Criminals hack into email networks to obtain knowledge about business payment systems, then trick company personnel into sending funds to their bank accounts.

Ransomware is a type of ransomware in which fraudsters encrypt computer systems in hospitals and public organizations and then demand money to unlock them.

Botnets are large-scale networks of compromised PCs that are used to automate large-scale attacks.

Analysis to action

"Criminals take advantage of differences in law enforcement capacities across physical borders, as well as vulnerabilities in cyber security across the area," said Craig Jones, INTERPOL's Director of Cybercrime.

University of Education,Winneba http://ir.uew.edu.gh

Mr. Jones continued, "INTERPOL's regional cybercrime strategy for Africa provides a robust framework for sharing intelligence and coordinating action to boost law enforcement response across Africa and beyond."

Criminal intelligence, law enforcement activities, regional capacity and skills, and corporate and public awareness initiatives are all part of the approach.

The African Cybercrime Operations Desk of INTERPOL will lead the implementation, working closely with important regional stakeholders such as the African Union and Afripol, law enforcement agencies, and the corporate sector. "Criminals take advantage of differences in law enforcement capacities across physical borders, as well as vulnerabilities in cyber security across the area," said Craig Jones, INTERPOL's Director of Cybercrime.

Mr. Jones continued, "INTERPOL's regional cybercrime strategy for Africa provides a robust framework for sharing intelligence and coordinating action to boost law enforcement response across Africa and beyond."

Criminal intelligence, law enforcement activities, regional capacity and skills, and corporate and public awareness initiatives are all part of the approach.

The African Cybercrime Operations Desk of INTERPOL will lead the implementation, working closely with important regional stakeholders such as the African Union and Afripol, law enforcement agencies, and the corporate sector.

It was acknowledged that the African Cyberthreat Assessment Report 2021 was developed as part of the African Joint Operation against Cybercrime (AFJOC), which is supported by the Commonwealth and Development Office of the United Kingdom (FCDO). With the help of the German Federal Foreign Office, INTERPOL's Support Programme for the African Union (ISPA)

University of Education,Winneba http://ir.uew.edu.gh

contributed to the report. The data and expertise of INTERPOL's commercial sector partners Group-IB, Kaspersky, Palo Alto Networks, and Trend Micro were used in the research (INTERPOL, 2021).

2.8 Cybercrime in Ghana

Cybercrime is a new phenomenon in Ghana, according to Warner (2011). In the years 1999 and 2000, cyber fraud became more common across the country. Card fraud was the most common kind of electronic crime during this time. Credit was initially offered through international hotel chains' buttons, which shared credit card information of Western guests with criminals. In some cases, Ghanaian con artists would take the value of Western credit cards, use them to purchase things on the Internet, and then return them to Ghana. Since 2004, the use of social engineering approaches to hypnotize potential victims has decreased online credit card purchases due to the introduction of new methods of internet fraud. According to (Burrell, 2008), the internet scam/cybercrime in Ghana is a supplement to a more compassionate approach. The statistics which covered the time 2006 to 2011 are presented in table 1 below.

Table 2.0.1: Cybercrime Review (2006-2011)

Cases reported	Frequency	Percentage
Cases refused	2	1.2
Cases sent to court	15	9.4

University of Education,Winneba http://ir.uew.edu.gh

Cases convicted	12	7.5
Cases acquitted	1	0.6
Cases awaiting trial	2	1.2
Cases closed	1	0.6
Cases under investigation	128	79.5
Total	**161**	**100.00**

Police around the country have documented a total of 161 occurrences of cybercrime. Out of this total, 1.2 percent were cases that police did not pursue due to a lack of data or proof. According to the data under evaluation, 9.4 percent of cases have been taken to court, while 7.5 percent of cybercriminals have been apprehended. Nonetheless, the fact that 79.5 percent of the cases are still being investigated is intriguing. This could draw attention to the CID staff's investigative limitations. The growing use of technology by criminals in areas such as "Sakawa" and other computer-assisted fraud means that any type of crime can be performed with a high level of secrecy, development, and exemption because it is a challenge for the authorities.

Police retrieved and seized two HP laptops, one iPad phone, seven jars containing leaves suspected to be India hemp, one Huawei turbo net, one itel turbo net, one MTN turbo net, one digital microscope, Samsung power bank, lightning system, and laptop charges, according to a Ghana web report dated October 15, 2021. On Wednesday, October 13, 2021, a team led by DSP Harold Opoku Yamoah, the Akyem Kwabeng district Police commander, detained the suspect David Egbert, 26.

"Cybercrime in Ghana has assumed a rudimentary form of internet fraud targeting unsuspecting foreigners, known as Sakawa or 419," according to the research. According to the report, the

University of Education,Winneba http://ir.uew.edu.gh

offenses involved credit card and advanced fee fraud, and they took advantage of internet users' vulnerabilities and gullibility (GhanawebNews, 2021).

2.8.1 Intentional Acts that Affect the Bank

A few people are keen to participate in crime on purpose when it is against someone else. In any event, many people are unaware that this will reflect poorly on the bank and could be considered bank fraud. Taking a bank account's credentials, shifting money from one account to another, or producing a negative influence on a bank's record could all be considered bank fraud, according to the Bank Fraud Statute. When the intention was to defraud an individual rather than a financial organization, charges of bank fraud are possible. The individual may then find himself in jail or facing hefty fines as a result of their actions.

2.8.2 Reportage on Cybercrime in the banking sector of Ghana

Ghana loses Gh¢30.1 million to bank fraud

The Bank of Ghana (BoG) said that fraud cases in the banking industry climbed from 1,002 in 2016 to 1,418 in 2017. The statistic represents an increase of 41.66 percent (Graphic Online, 2018). The entire sum recorded for fraud or attempted fraud was around GH190.4 million, according to the BoG. (Graphic Online, 2018). GH160.30 million, or 84 percent of the entire value, was recovered, whereas GH30.1 million, or 16 percent, was reported as a loss. Officials from the Economic and Organized Crime Office (EOCO), the Bank of Ghana, National Security, the Ghana Police Service, and the Ghana Association of Bankers attended the event. This was revealed during a press conference following the release of the BoG's 2017 State of Banking Sector Fraud Report. The report was a compilation of fraud reports made by banks at the end of

University of Education,Winneba http://ir.uew.edu.gh

each month. It indicates that there were 235 registered financial institutions, made up of non-bank financial institutions (NBFIS), rural and community banks, and commercial banks, with only 58 reported cases of fraud. He noted that the distribution of reported fraud for 2017 indicated that 51.13 percent of fraud incidents were reported by the NBFIS, while 33.15 percent and 15.72 percent were reported by commercial banks and rural and community banks, respectively.

2.8.3 Banking Industry Fraud Report in Ghana

The total number of fraud incidents reported in 2020/2019 is shown in Table 2.1. In 2020, there were 2,670 fraud reports filed, up from 2,311 in 2019, reflecting a 15.5 percent rise in the number of fraud reports submitted to the Bank year over year. In 2020, a number of fraud categories saw an upsurge. Fraudulent withdrawals, E-Money Fraud, and ATM/POS Fraud are the most prominent fraud types recorded in 2020, in terms of occurrence and/or loss to the banking system (BankofGhana, 2021).

Fraudulent Withdrawals had the highest rate of increase in the year under review, according to the BoG fraud report on the banking industry for the period 2020. The number of fraudulent withdrawals climbed from 16 in 2019 to 177 in 2020, indicating an increase.

University of Education,Winneba http://ir.uew.edu.gh

Fraud Type	January to December 2019	January to December 2020	Y-o-Y Change in 2020 (%)
Suppression	1774	1958	10.37
Fraudulent Withdrawals	16	177	1,006.25
ATM POS	110	168	52.73
Forgery and manipulation of documentation	157	151	(3.82)
e-money	14	126	800.00
Cyber - email fraud	112	28	(75.00)
Lending/credit fraud	36	18	(50.00)
Cheque Fraud	40	16	(60.00)
Remittance	8	10	25.00
Others	29	9	(68.97)
Burglary	7	6	(14.29)
Impersonation	8	3	(62.50)
Total	2311	2670	15.5

Figure 3 Count of Bank Fraud Cases in Ghana

Source: Bank of Ghana 2020 Report

2.8.4 Cyber fraud

According to the data, cybercrime fraud cases had the greatest value of attempted fraud, totaling GH 110,865,960, with less than one percent resulting in a loss. She defined cybercrime as external parties gaining illegal access to financial institutions' banking systems, email fraud, and crimes committed through internet banking and other localized payment and mobile banking services. Mrs. Poku believes that the rise in cyber fraud is due to a deteriorating cybersecurity environment, the active presence of fraud syndicates in banks and telcos, and lax regulations over the protection of banking data.

University of Education,Winneba http://ir.uew.edu.gh

Figure 4 Fraud types and Gross Loss

Cash suppression

According to the report, the most documented form of fraud among the NBFIS was the suppression of deposits and cheques, with attempted fraud totaling roughly GH15.1 million. This form of fraud, however, resulted in a loss of approximately GH11.3 million. It claimed that internal and contract employees, particularly tellers and mobile cash mobilization officers, were responsible for 90% of the crimes recorded by the NBFIS (BoG, 2021).

Why do banks commit so much fraud?

Why are banks so easily defrauded? I'm not talking about bank fraud, but rather fraud done by banks or fraud assisted by bank behaviour. U.S. officials penalized the Toronto-Dominion Bank's U.S. branch $52.5 million last week for its role in a $1.2 billion Ponzi scam run by a lawyer

University of Education,Winneba http://ir.uew.edu.gh

named Scott Rothstein. The bank ignored customer account activity that "repeatedly generated signals in the Bank's anti-money laundering monitoring system," according to the US Department of the Treasury. The bank "defrauded investors by generating a series of deceptive documents and making false assertions about accounts that Rothstein had at the bank and used to perpetuate his scheme," according to the Securities and Exchange Commission. The Royal Bank of Canada agreed to pay $17 million last year.

Furthermore, we must not neglect the participation of banks, especially Canadian banks, in the financial crisis of 2008, which was caused by the sale of subprime mortgages and other kinds of bad debt that were turned into investment products and peddled to an unwitting public. We also can't ignore the Libor scandal's interest rate manipulation. Banks knowingly disclosed incorrect borrowing rates, according to Bloomberg Businessweek, affecting the "worth of trillions of dollars in derivatives contracts, mortgages, and consumer loans." These are just a few examples of recent bank misbehavior. It's almost as though a virus has infected banks all around the world. Our ostensibly conservative Canadian banks have not proven to be immune. This isn't the fault of renegade employees. There are just too many events occurring.

Why commits fraud?

The perpetrators do not necessarily have the same identities but have similar characteristics. Many people are driven to the fraud cause simply out of an interest in what they don't have, perhaps what they want to own. In addition to individual intentions to fraudulently acquire the things that they may need, the things that they do not have and, depending on the influence of the

University of Education,Winneba http://ir.uew.edu.gh

environment, they find that there is also a great desire for a group of people or clans that have group desires to obtain earnings for fame. , property ownership, being financially sound, etc.

Five Most Common Types of Banking Fraud

As banks open to new computerized channels, fraudsters may exploit security loopholes that pass undetected by banks and end up causing a noteworthy consistency fine or data loss. Luckily, the digitization of banking administrations additionally achieves new technological solutions ready to handle current security challenges and recognize dubious conduct efficiently, helping banks to shield digital data from fraud.

i. Money laundering

Money laundering is the main source of compliance fines for financial institutions. Banks can utilize smart transaction segmentation to spot money laundering endeavors immediately and abstain from being fined. Money laundering is the way toward hiding the inceptions of cash got wrongfully by going through an intricate succession of banking moves or business exchanges. The general plan of this procedure restores the cash to the launderer in an obscure and indirect way (Oxford English Dictionary, 2005). A matter of crime is accounting for returns without generating alerts from law enforcement agencies. Much time and effort could be devoted to systems that enhance the protected use of these returns without raising undesirable doubts. Updating stories methodologies is mainly called money laundering. Once the cash has been laundered, it can be used very well for genuine purposes. The law enforcement offices of various neighborhoods have established sophisticated systems with the ultimate goal of distinguishing suspicious transactions or activities, and many have established international aid plans to help

University of Education,Winneba http://ir.uew.edu.gh

each other in these businesses. In various legitimate and administrative settings, the term "money laundering" has been combined with different types of budgetary and commercial crimes, and is sometimes even more used to incorporate abuse of money financial systems (including things, for example, securities, digital currencies, credit cards, and traditional currency).

How does it impact the bank?

The effect of such events can be destroyed, not least the financial consequences. By the method, for instance, one just needs to look at a portion of the ongoing prominent cases to hit the news, for example, those at Société Générale (a €4.9 billion exchanging fraud)1, RBC ($1.1 million theft)2 and Lloyds (£2.4 million receipt fraud). Just as the tremendous financial losses, the harm to the reputation of the bank can be critical. Bank representatives are trusted and regarded people – and any recommendation that they may act deceitfully brings to scrutinize the relationship that people will have with that organization. Put essentially, clients will lose confidence in their bank if its staff can't be trusted to safeguard their accounts.

ii. Credit card fraud

That type of fraud is typical, but new tools using machine learning algorithms for risk management shed light on the way to fix the problem. Financial organizations used to rely on linear algorithms to distinguish between suspicious and large transactions. Today, banks are exploiting more developed algorithms that separate acceptable and potentially fraudulent transactions. They put positive exchanges on the express path and run increasingly advanced algorithms on clients that seem to be progressively risky. These algorithms are accessible to banks due to the expanded registration limit of cloud innovations. Credit card fraud is a broad

University of Education,Winneba http://ir.uew.edu.gh

term for theft and fraud sent using or including a payment card, for example, a credit or debit card, as a fraudulent source of funds in a transaction. The reason could be getting unpaid products or getting unapproved assets from an account.

Credit card fraud is also subordinate to fraud. As indicated by the Exchange Commission of the US Government. While the pace of identity theft remained uninterrupted in the mid-2000s, it expanded by 21 percent in 2008 (The Encylopedia , 2018). Be that as it may, credit card fraud, the crime that many people associate with identity theft, declined as a level of all identity theft complaints for the sixth consecutive year. Although the frequencies of fraud with credit cards are restricted to approximately 0.1% of all card transactions, they have caused great financial losses since the fraudulent transactions have been transactions of great value. In 1999, of 12 billion transactions made annually, approximately 10 million, or one in 1,200 exchanges, ended up being fraudulent. Furthermore, 0.04% (4 out of 10,000) of all dynamic month-to-month records were fraudulent. Even with colossal volume and increased value in credit card transactions thereafter, these extensions have remained the same or decreased due to refined fraud identification and avoidance systems. Current fraud detection systems aim to avoid one-twelfth of one percent of all prepared transactions that still translate into billions of dollars in losses.

Compromised accounts

Card data is saved in various ways. Card numbers – officially the Primary Account Number (PAN) – are regularly embossed on the card, and an attractive stripe on the back contains the information in a machine-readable format. Fields can differ, yet the most widely recognized include:

- Name of the cardholder

University of Education,Winneba http://ir.uew.edu.gh

- Card number
- Expiration date
- Verification/CVV code

2.9 Conceptual Framework

This outline underneath demonstrates a straightforward process for connecting the elements of cybercrime dynamics. Figure 5 below indicates the variables understudy for this work. The variables are facets of cybercrime, threats of cybercrime, effects of cybercrime, and the mitigation of cybercrime in Ghana.

The facets of cybercrime will unearth the various types of cybercrime that are common in Ghana. The threats cybercrime imposes on individuals and organizations will be identified.

The relationship between facets, threats, effects, and the mitigation of cybercrime will be addressed as depicted in figure 5.

University of Education,Winneba http://ir.uew.edu.gh

Figure 5 Conceptual Framework of the study

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

Scientific research implications are beneficial to the extent that the most capable methodologies and organizations recognize them in the planning and execution of field operations, similar to data analysis (Kumekpor, 2002). Croswell (2013) further explained that the research approach chosen does not influence the research design, but it does allow the researcher to consider how each approach can enhance or limit their research. In general, there are three reasons why social research should be promoted. One of them is to provide an explanation. A census, for example, is a representation of the population's demographics. The following reason for existence is to clarify things, and a study conducted in this manner as result of this is a good example.

3.2 Research Design

The term "research design" refers to a method of researching a study that spans the choice from a broad assumption to a crucial method of data collecting and analysis (Creswell, 2009). The qualitative approach is appropriate for exploratory investigations because the population under examination is covered, like in this case where the research region is new, doubtful, or concentrated on criminal behaviour. Due to their social status, some unfortunate victims are embarrassed to report the event to the authorities (Warner, 2011). The methodology directs the research and minimizes the need for additional data (quantitative or subjective) within the scope of the study. The settling procedure plays a significant role in the most common way of improving data analysis comprehension. As a result, (Morse, 1991) argued that essentially, a qualitative approach is required.

University of Education,Winneba http://ir.uew.edu.gh

3.3 Study Area

The Kumasi Metropolis is located in the central part of Ghana's Ashanti region. Because of its unique geographic location, it is easily accessible from all parts of the country. Kumasi is the administrative capital of the Ashanti region and the second-largest city in Ghana. It is a fast-growing metropolis, with an estimated population of 3,630,000 people and an annual growth rate of over 4.01 percent per Anum according to Ghana Population and Housing census, 2021. The Kumasi Metropolitan Area is located approximately 270 kilometers north of Accra, Ghana's national capital, and 120 kilometers southeast of Sunyani, the capital of the Bono Region. It is located between Latitude 6.35° N and 6.40° S and Longitude 1.30° W and 1.35° E and is elevated 250 to 300 meters above sea level. The Central Business District (CBD), which includes the Kejetia market tagged " Kejetia Dubi", the Central Market, and the Adum Shopping Center, is the first and most important district. Suame Magazine (Vehicle Repair Approach), Kaase / Asokwa Industrial Area and Anloga are some of the other places that contribute monetarily to the economy.

The research was carried out in Kumasi, Ghana. The bulk of cybercrime incidents happened in this region, according to preliminary data acquired by the Police Service's Criminal Investigation Department (CID), and in most cases, it is indicated in media reports that they have a high omnipresence rate of cybercrime. The area was designed to allow the investigator to communicate with the various police units combatting cybercrime in Ghana. Kumasi is also the Akan ethnic group's regional capital. The Ashanti region's capital, Kumasi, is the most populous city. It has a population of 3,630,000 people according to the 2022 census. Depending on the rate of development, it was having a population of 3,490,000 as of 2021.

University of Education,Winneba http://ir.uew.edu.gh

3.4 Sampling Techniques

The researcher employed two non-probability sampling approaches to choose the respondents, intentional and snowball, because the population substitution (Victims and Offenders) was reserved. The snowball test, often known as "chain sampling," is a particularly plausible selection strategy for identifying individuals who would be difficult to find using other methods (Hennink, Hutter, & Bailey, 2011). It suggests that the researcher can identify a person from a specific social network and use the snowball's impact to track down additional people like friends, family, coworkers, and associates to identify possible respondents. Furthermore, because the interview was conducted face-to-face, pleasant ties were formed, and a few interviewees were encouraged to connect the interviewer with other social networked persons. Furthermore, the use of social media was beneficial.

3.5 Sample Size

A total of 30 people took part in the survey. Twelve bank employees, six victims from Kumasi's Central Business District, and twelve police officers were recruited from four units at the Kumasi CID office who had prior experience with internet fraud. Cyber Crime Unit, Documentation and Visa Fraud Section (DVS), Intelligent Unit (IU), and Commercial Crime Unit are the offices involved (CCU). From each unit, two officials were picked. The four senior cops in charge of these units were specifically chosen to add to the dialogue. The assumption is that the greater a person's rank, the more information they can access at work. Four more employees were picked at random from lower-level roles to offer their ideas and experiences.

University of Education,Winneba http://ir.uew.edu.gh

Because of the principle of saturation, the researcher chose 12 banking respondents for the number of respondents. It's the time in the data collection process when no fresh or important information emerges from the interviewees (Bryman, 2008). "In the wake of reaching information saturation," (Hennink, Hutter, & Bailey, 2011) said, "additional data-collecting exacerbates the excess because the purpose of recruiting is to hunt for variation and setting of member participants as opposed to countless members with similar encounters." Although the interviews took place in diverse parts of Kumasi, the investigator realized after meeting the Ninth respondent that the succeeding candidates had nearly identical responses to the questions posed to them.

At the near stage, serious perusing happened while the researcher skimmed the transcripts by moving forward and backward between the recognizable proof of similarities and contrasts between rising classifications. For saturation, in the wake of arriving at the ninth respondent, I understood a large portion of the respondents continued rehashing in the consequent interviews; no new class was discovered from the codes and the variety for existing classifications additionally stopped rising. So further meetings would essentially include time and cost without adding to the scope of techniques effectively recognized. In this way, (Corbin & Strauss, 2008), inferred that the number of participants in a qualitative study is adequately guided by the decent variety of the data gained. Internet fraud casualties were hard to reach. The data assembled from the CID uncovered that unfortunate casualties are normally prominent people or rich persons who can't confront the humiliation of individuals realizing that they have been duped. Also, foreign victims who needed to seek after the case was being prompted by their Envoys to haul

University of Education,Winneba http://ir.uew.edu.gh

out of the absence of trust in the Ghanaian legal system, which has been spoiled with corruption and undue delay of cases. These elements may have been represented by the low reaction rate.

3.6 Sources of Data Collection

The study included both secondary and primary data. To review the literature, secondary information was gathered from books, articles, papers, organization reports, and internet sources. These were examined in Chapter 2 to show that cybercrime is a worldwide phenomenon. Primary data was also acquired through preliminary fieldwork and face-to-face interviews.

Table 3.0.1: Demonstrating the order of respondents and the kinds of information produced from them.

Summary of Data Source

CATEGORIES OF RESPONDENTS		**NUMBER**	**(%)**	**SAMPLING TECHNIQUES**	**TYPE OF DATA COLLECTED**
1	Police personnel (key informants)	12	40%	Purposive	Qualitative
2	Banks / Victims	12	40%	Purposive	Qualitative
3	Public / Victims	6	20%	Snowball	Quantitative & qualitative
Total		30	100		

University of Education,Winneba http://ir.uew.edu.gh

3.7 Data Collection Technique

The data was collected for 10 weeks (i.e. from May 2021 to February 2022). Three sets of interviews were conducted for the selected respondents; victims, the police, and the banks. (Hennink, Hutter, & Bailey, 2011), exhorted that, the focal point of the research in the qualitative study is to increase the definitive understanding of a certain phenomenon, to recognize the socially developed implications of the phenomenon and the environment in which the phenomenon occurred. To achieve this, an in-depth interview method (one-to-one) was used with the interviews used to collect a detailed understanding of the research problem of the participants studied.

3.8 Research Instruments

An interview guide was one of the most important tools used to acquire information. The meeting planner anticipated a face-to-face meeting between the investigator and each of the participants. Because the population is unknown, individual discussions established a strong rapport, ensuring high-quality responses. By following up on queries to clarify suspicious arguments on cybercrime, the questioner was able to explore deeply into respondents' convictions, states of mind, and internal contacts, thanks to the adaptive idea of the meeting aide.

.

3.9 Data Analysis

The qualitative analysis comprises a disclosure approach that allows the researcher to remain close to the facts and construct a proof-based understanding of the study topics. The Grounded qualitative procedure was applied, and a substantial number of the procedures were explained during the saturation process, as previously stated.

University of Education,Winneba http://ir.uew.edu.gh

When the data was acquired, each of the in-depth interviews was transcribed. It allowed me to identify new issues that filtered into the interviews that followed, resulting in more significant data in the data acquired as the project progressed. Codes were identified from the readings, and they involved ideas and a viewpoint held by the respondents. According to Strauss (1987), "the perfection of qualitative research depends in large measure on the brilliance of coding."

3.9 Ethical Considerations

According to Kumekpor (2002), the respondents are the most significant part of the study, and everything feasible should be done to alleviate their anxiety and terror. Neuman (2003) goes on to say that "morality described what is or is not authentic to perform, or what good research the researcher should contain." He also emphasized that morality begins and ends with the investigator's integrity and values. (Bryman, 2008) further cautioned that the essential moral criteria of social research are as follows: never force anybody to participate; participation must always be voluntary. Individuals must grasp what they are encountering to become engaged and make educated judgments. Consent alone is not sufficient.

3.9.1 Problem Encountered on the Field

A notable problem of the study was how much the success of the research hinged on the willingness of respondents to collaborate with the researcher and provide detailed responses. In any scenario, few people would refuse to be recorded because their voices might be easily identified. This meant the researcher would have to take a lot of notes, which slowed down the interview's flow and tempo. Worse, the criminals questioned whether the researcher was collecting data for security authorities. Nonetheless, this impediment was overcome by the

University of Education,Winneba http://ir.uew.edu.gh

consolation of the most severe classification and the employment of pen names to communicate with respondents to conceal their true identities. Similarly, interviews were usually conducted away from the office.

Another flaw was that all of the victims of cybercrime interviewed were Ghanaians. Despite this, record checks revealed that the majority of the unlucky victims were from the outskirts of Ghana. Because the police had lost contact with the exploited persons, the researcher's efforts to locate them proved futile. Furthermore, those who reported the matter to the Ghana police chose to remain silent based on instructions from their ministers and high officials, owing to a lack of trust in the Ghanaian criminal justice system.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSION

The data received from the qualitative interviews are analyzed in this chapter. The study objectives were met by the analysis. To answer the various objectives, a distinct collection of respondents was used. As a result, each aim has an answer derived from a variety of sources.

4.1 Demographic background of Respondents

The researcher gathered data for this project by drawing on the expertise of twelve (12) Ghana Police Service officers, twelve (12) banking professionals from various banks, and six randomly selected respondents from Kumasi Metropolitan Assembly's Central Business District, Adum.

4.1.1 The Ghana Police Service Demography of Respondents

Twelve (12) Ghana Police officers were used, and they were chosen from four units at the CID office in Kumasi who had prior experience with computer fraud. Cyber Crime Unit, Documentation and Visa Fraud Section (DVS), Intelligent Unit (IU), and Commercial Crime Unit are the offices involved (CCU). There are four (4) females and eight (8) males in this group.

However, two officials were chosen at random from each unit. The numerous officers in charge of these units were hand-picked to add to the dialogue. The belief that the higher the rank, the more resourceful one can be at work influences the selection process. Years of security service experience range from three to twenty years. Table 4.1 below was the distribution of the demographic background of respondents.

Table 4.0.1 Demography of Respondents from Ghana Police Service

University of Education,Winneba http://ir.uew.edu.gh

Respondent	Age	Gender	Rank	Unit	Years of service
1	44	Male	SP	Cybercrime	20
2	29	Female	Sergeant	Cybercrime	5
3	28	Male	Corporal	Cybercrime	4
4	44	Male	ASP	Commercial Crime	16
5	36	Male	C/Insp.	Commercial Crime	12
6	33	Male	Inspector	Commercial Crime	9
7	40	Male	ASP	Document Visa Fraud	16
8	33	Female	Inspector	Document Visa Fraud	9
9	27	Female	Corporal	Document Visa Fraud	3
10	35	Male	ASP	Intelligent Unit	12
11	31	Female	Sergeant	Intelligent Unit	7
12	43	Male	Sergeant	Intelligent Unit	8

Source: Field Survey 2021

Age Distribution

The ages of the respondents start from 27years to 44years. The distribution indicates two senior officers are 44years, 40, and 35years old, all in the rank of SP and ASP, and the rest are just an officer each (27, 28, 29,31,33,36, and 43). Averagely the female officers are younger than the male officers.

University of Education,Winneba http://ir.uew.edu.gh

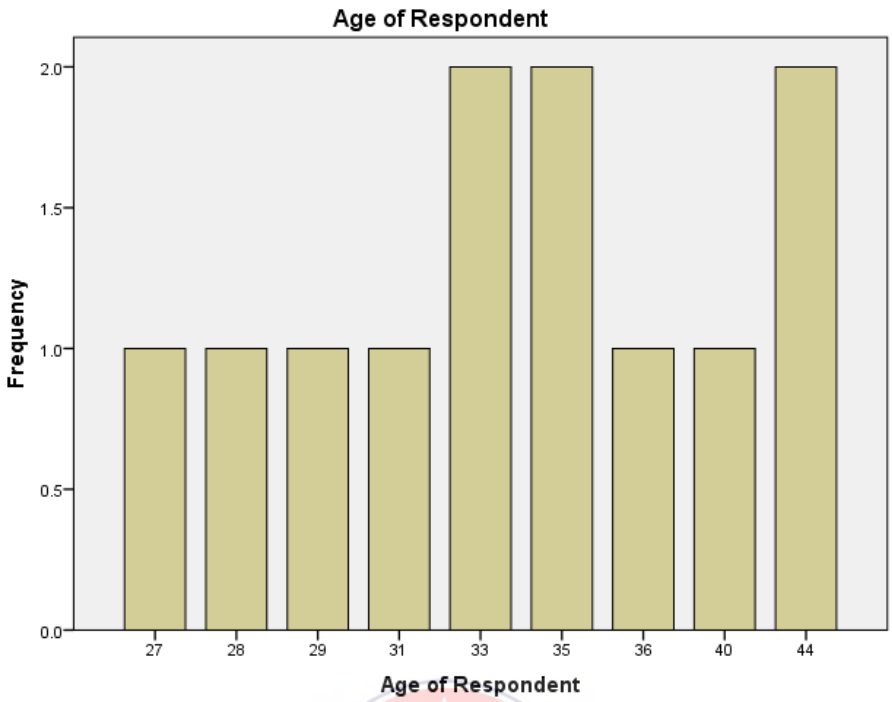


Figure 6: Age Distribution of Respondents

Rank Distribution

The senior-most among the workforce were of the rank Superintendent of Police (SP), three (3) Assistant Superintendent of Police (ASP), three (3) Inspectors of which one (1) was a Chief, three (3) Sergeants, and two (2) Corporals.

University of Education,Winneba http://ir.uew.edu.gh

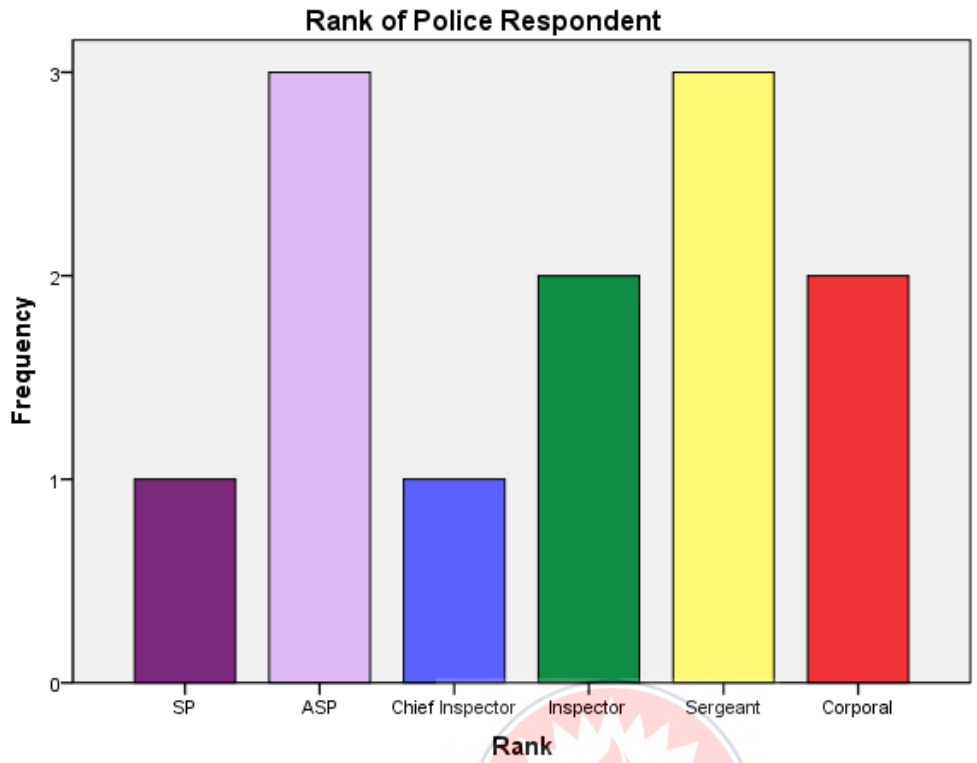


Figure 7: Rank Distribution of Police Personnel

Source: Field Survey 2021

Unit Distribution

All four units were chosen from the Criminal Investigation Department of the Ghana Police Service. Each of the following units had three (3) officers purposively chosen: Cyber Crime Unit, Documentation and Visa Fraud Section (DVS), Intelligent Unit (IU), and Commercial Crime Unit (CCU).

University of Education,Winneba http://ir.uew.edu.gh

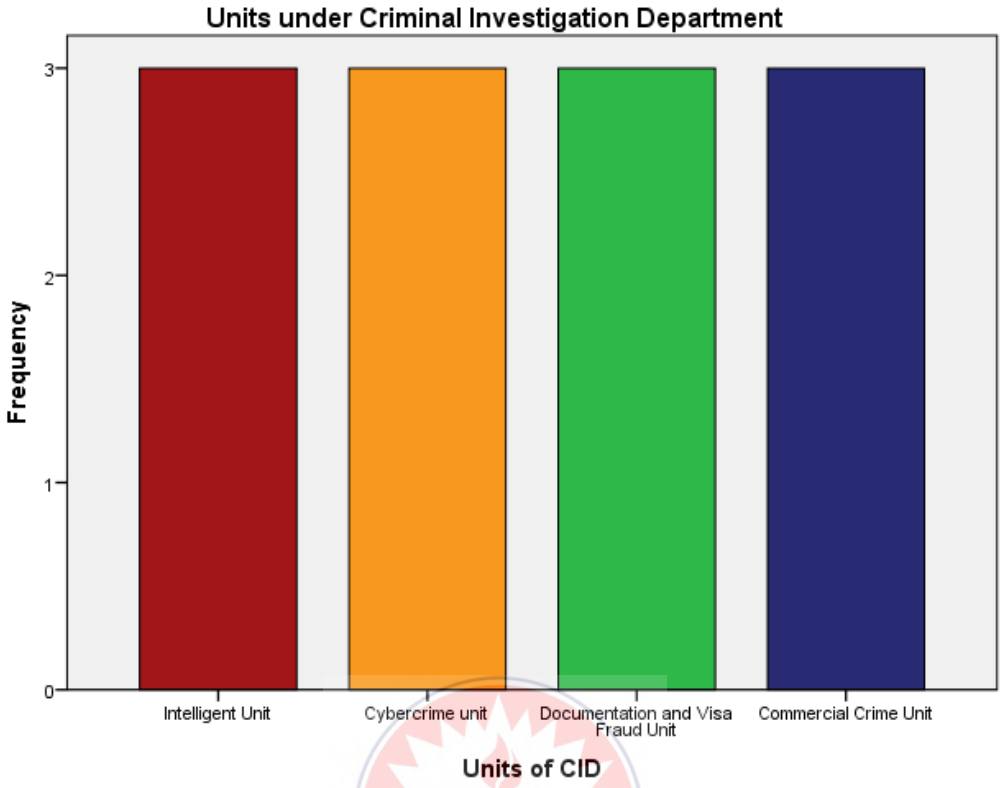


Figure 8: Units Distribution of CID

Work Experience

The most experienced among the selected official had served in the Ghana Police Service for 20years at least 3 years.

University of Education,Winneba http://ir.uew.edu.gh

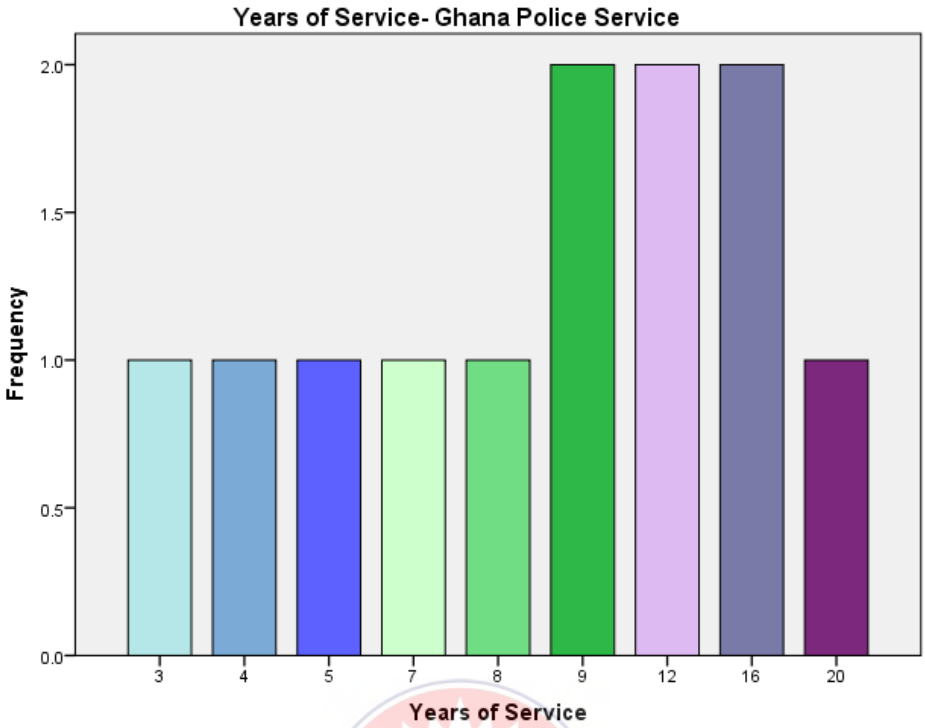


Figure 9 Years of Service

Source: Field Survey 2021

Although there were challenges of delaying response to be interviewed due to the exigency of their service to the security needs of the Region, the respondents were very cordial, respectful and prudence in their response to every question.

University of Education,Winneba http://ir.uew.edu.gh

4.1.2 The Demography of Respondents from the Banking Sector

Data collected from the banking sector indicated that out of the twelve respondents, six female and male each were involved. This further indicates that the ages were between 28 and 53 years. The oldest person is 52 and the youngest is 29 years of age. These respondents cut across nine (9) commercial banks, one (1) central bank, and one (1) mini-central bank. The commercial banks are Access, ADB, GCB, ABSA, CBG, First Atlantic, Ecobank, GTB, and Fidelity. The central bank is the Bank of Ghana and APEX bank a mini central bank for Rural and Community banks in Ghana.

However, these respondents hold various positions in their respective banks, of which, three (3) were Bankers and Relations Mangers each, two (2) Accountants, two (2) Investment Officers, one Credit Officer, and one Branch Manager. They have reasonable work experience from 3 years to 26years. Tables 4.3, and 4.4 show a summary of the demographic details of the respondents in the banking sector. Figure 13 presents a pictorial distribution of the various banks visited during the survey.

Table 4.0.2 Demography of Respondents from Banks

Respondent	**Age**	**Gender**	**Position**	**Banks**	**Years of service**
1	52	Male	Accountant	Ecobank	26
2	48	Female	Banker	GCB	23
3	44	Male	Branch Manager	GT Bank	18
4	42	Male	Banker	APEX Bank	16
5	40	Male	Banker	Bank of Ghana	16
6	35	Female	Accountant	Ecobank	8
7	35	Male	Investment Officer	ABSA	8

University of Education,Winneba http://ir.uew.edu.gh

8	35	Female	Relation Manager	Fidelity Bank	9
9	32	Male	Relation Manager	CBG	6
10	31	Female	Investment Officer	First Atlantic	6
11	30	Male	Credit Officer	Access Bank	4
12	29	Female	Relation Manager	ADB	3

Source: Field Survey 2021

Age Distribution

The ages of the respondents start from 29years to 52years. Three Banking officers were 35years, 52years,48years, 44years,42years, 40years, 33years, 32years, 31years,30years, and 29years were just an officer each. Averagely the female officers are younger than the male officers.

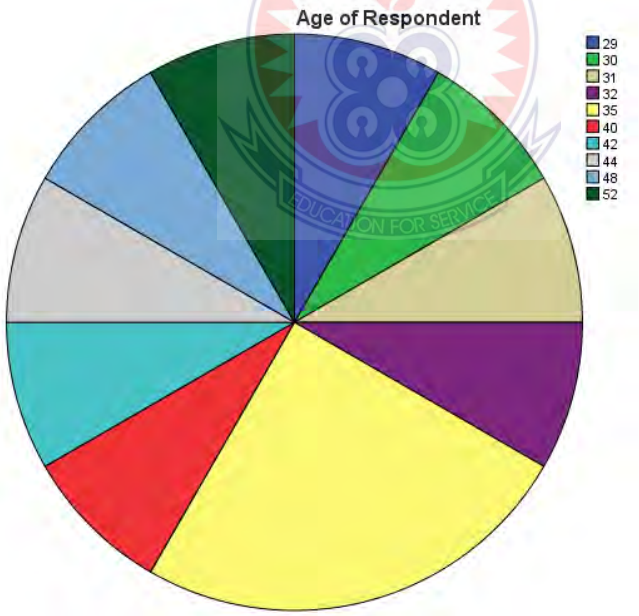


Figure 10 Age of Bank Staff Respondents

University of Education,Winneba http://ir.uew.edu.gh

Gender

The data collated from the various banking institution indicate that six (6) female and male responded to the questions. Figure 11 below is the pictorial representation of Gender distribution in a pie chart.

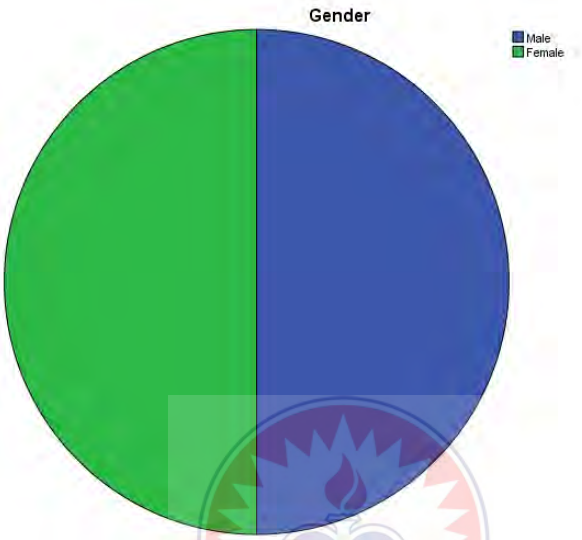


Figure 11 Gender of Bank staff

Position

Out of the twelve (12) respondents, three (3) were Relation Managers and Bankers, two (2) were Accountants and Investment Officers, and one each for Credit Officer and Branch Manager.

University of Education,Winneba http://ir.uew.edu.gh

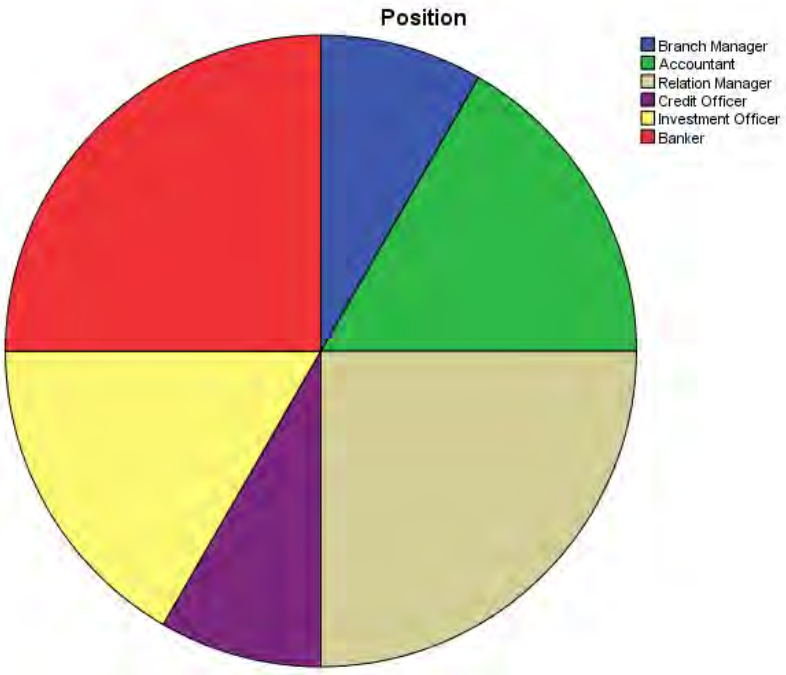


Figure 12 Position held by Respondent

Banks

Figure 13 below gives a forecast of the selected banks for the survey. The banks were 11 banks, 2 respondents from Ecobank, 1 respondent each from the following banks: ABSA, Access Bank, APEX Bank, Bank of Ghana, Consolidate Bank Ghana (CBG), Ecobank, Ghana Commercial Bank (GCB), and Guaranty Trust Bank (GTB).

University of Education,Winneba http://ir.uew.edu.gh

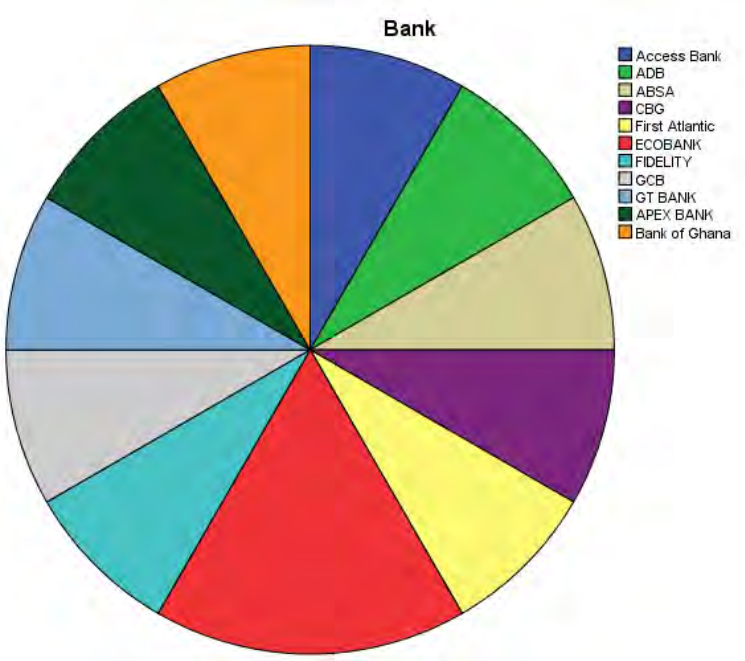


Figure 13 Banks of Respondents

Years of Working Experience

In analyzing the working experience, the minimum years of experience were 3 years and the maximum was 26years. The average years of service are 11.91 which is approximately 12 years.

University of Education,Winneba http://ir.uew.edu.gh

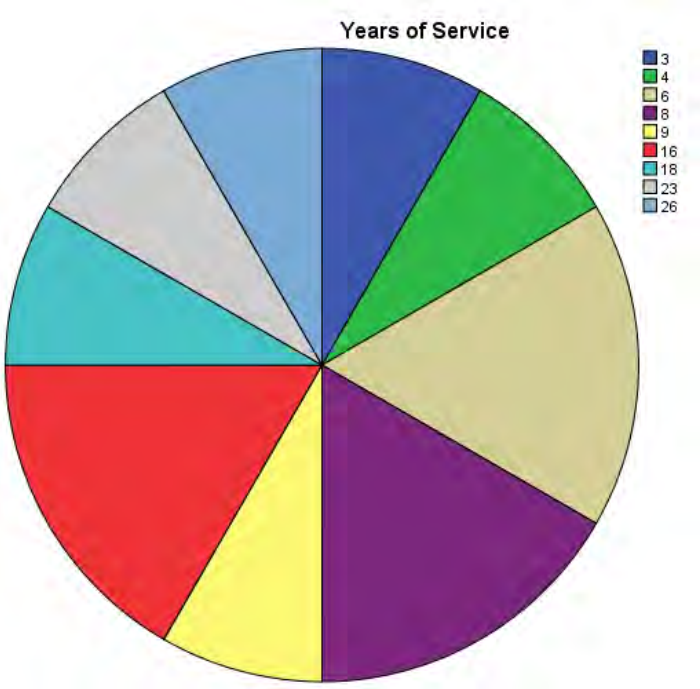


Figure 14 Years of Experience

4.1.3 The Demography of Respondents from Central Business District- Adum

Age Distribution

The ages of the respondents start from 22years to 44years. The age distribution of the Central Business District (CBD) respondents were 44years,42years, 30years, 27years, 24years, and 22years were just an officer. Averagely the female respondents are younger than the male respondents.

Gender

The data collated from the individuals within the CBD (Central Business District) indicate that four (4) female and two (2) male responded to the questions. This presents a gender ratio of 1:2. A male maps unto 2 females.

University of Education,Winneba http://ir.uew.edu.gh

Type of Employment

Out of the six (6) respondents, one (1) was a Civil servant, one (1) businessman, three (3) graduates unemployed, and one (1) tertiary student.

4.1.4 Summary of the Demography of all Respondents

In total, the population of the respondent is thirty (30), which comprise twelve (12) from the Banking Sector, twelve (12) from the Ghana Police service, and six (6) victims from the general public. this constitutes a percentage of 40, 40, and 20 respectively.

The average age of respondents of all the various categories from Ghana Police, Banks, and Victims from the general public is 36years.

However, twenty-five (25) of the respondents are gainfully employed in both public and private sectors, one (1) self-employed, three (3) graduate unemployed, and one (1) student. This was so because of the target grouping of the respondents.

Table 4.0.3 Type of Employment of Respondents

Type of Employment	Number	Percentage
Public sector	15	50%
Private sector	11	37%
Unemployed	3	10%
Student	1	3%

Source: field survey (2021)

University of Education,Winneba http://ir.uew.edu.gh

4.2 what are the Facets of Cybercrime in Ghana?

This section was used to assess the validity of the first objective of this study. Research question 1 is what are the facets of cybercrime in Ghana? The data collected and processed was to learn about the aspects or types of cybercrime in Ghana. Background information on the various types of cybercrime was gathered to assess their impact on Ghana's banking system. The data obtained on the various aspects of cybercrime from all three categories of respondents were examined using descriptive statistics. The response from the three categories is presented in table 4.4 below.

Table 4.0.4 Facets of Cybercrime Respondents

Variable / Factors	GPS	Banks	CBD	Total	%
Mobile Money	12	12	6	30	100
Money laundering	12	12	6	30	100
Credit card Fraud	12	12	6	30	100
Identity Theft	12	12	6	30	100
Accounts Takeover	12	12	6	30	100
Investment fraud	12	12	6	30	100
Relationship fraud	12	12	6	30	100
Cheque fraud	5	1	3	8	27
Phishing	12	12	6	30	100
Hacking	12	12	6	30	100
Sales and Promotional deals	11	11	6	28	93
Online purchase fraud	12	12	6	30	100

Source: Field Survey 2021

University of Education,Winneba http://ir.uew.edu.gh

Hacking, Phishing, Relationship fraud, Internet purchase fraud, Investment fraud, Account takeover, Identity theft, Credit card fraud, Money Laundering, and Mobile money fraud were all identified as characteristics of cybercrime by 100 percent of the respondents.

However, 93 percent of the respondents agreed that online purchase fraud is a type of cybercrime, while just 27% agreed that check fraud is a type of cybercrime.

Cheque fraud, in particular, was not completely recognized as a kind of cybercrime because it was not considered to be computer-based. According to the Field study (2021), respondents said in their interview that cheque fraud can be started with the use of a computer, but that the theft of a cheque leaf and falsifying the signature of the account holder's authorized signatory are the most common methods.

Finally, the acceptable aspects or types of cybercrime are as follows: ***Hacking, Phishing, Relationship fraud, Investment fraud, Account takeover, Identity theft, Credit card fraud, Money Laundering, Mobile money fraud, and online purchase fraud.***

Eventually, research question 1 has been addressed, identifying the facets of cybercrime that are common in Ghana.

4.3 What are the cybercrime threats faced by most Banks in Ghana?

The purpose of this inquiry was to determine which cyber-threats do most banks faced in Ghana. Once those threats are identified, then a pancea can be devised. Cybercrime in banking cannot be minimized or prevented if the underlying dangers are unknown. There are a variety of cybercrime dangers that are previously known, but the purpose of this survey is to determine which ones are most relevant to the banking industry in Ghana. According to the interviewees' comments, banks are in jeopardy for the simple reason that, in this period of huge information technology growth, computer applications for business have become accessible. "No one is

University of Education,Winneba http://ir.uew.edu.gh

secure when interacting with computers and networks," said one interviewee, because they believed "people are more equipped with information."

Descriptive statistics were used with a focus on standard deviation, to identify the common cybercrime threats that are related to Ghana's banking industry. The table 4.5 below is presentation of information of the processed data collected from the field survey.

The letters used in table 4.5 are S.A = Strongly Agree, A= Agree, N=Neutral, D= Disagree and S.D = Strongly Disagree.

Table 4.5 Responses to the threat of Cybercrime in Banking

Variables or Factors	S.A	A	N	D	S.D	Total
Digital extortion	9	12	3	6	0	30
Cash is suppressed in cybercrime	13	14	2	1	0	30
Online scam	12	16	2	0	0	30
Business email compromise	12	14	4	0	0	30
More unemployed graduate youth	4	7	6	7	6	30
Unsecure website of banking institutions	8	16	6	0	0	30
Ransomware	12	16	2	0	0	30
Insatiable crave for more money	10	10	5	0	5	30

4.3.1 What are the cyber fraud threats in banking?

The concept of variability among the data collected from all respondents was used to gauge the spread of prevalent cybercrime threats in the banking industry. To determine which characteristics are significant to banking, a Likert-style inquiry was utilized to collect data from respondents with prevalent cybercrime threat variables.

University of Education,Winneba http://ir.uew.edu.gh

The identified threats of cybercrime in the banking sector are online scams. Digital extortion, Ransomware, Business email compromise, and Botnets.

Networks of compromised machines are used as a tool to automate large-scale cyberattacks to steal the identity of an account holder, and make a transaction.

Fake emails or text messages claiming to be from a legitimate source are used to trick individuals into revealing personal or financial information. Victims can be tricked into sharing sexually compromising images that are used for blackmail.

Criminals hack into email systems to gain information about corporate payment systems, then deceive company employees into transferring money into their bank accounts.

Cybercriminals block the computer systems of hospitals and public institutions, then demand money to restore functionality;

In conclusion, it can be deduced from the preceding remarks that banks are not safe, particularly in this era when banking has grown competitive and the need to attract more consumers has resulted in the diversification of businesses. As a result, cyber fraud has infiltrated banks that are lacking in network banking operations. "Cyber fraud is a hazard not only to the owners and staff of the banks but also to the state and the clients," one responder said, illustrating how unstable this sector has become. It's too horrible to hear about bank closures here and there, which result in a massive loss of capital and jobs" (Field Interview, 2021).

4.3.2 How cyber fraudsters' operations have affected banking of late?

Cyber fraud in banking without a doubt, has the potential to harm the bank's progress. As a result, one responder stated, "The Bureau of Cybercrime should combat fraudsters' operation by

University of Education,Winneba http://ir.uew.edu.gh

guaranteeing excellent security systems" since "it leads to bank closures, which denies the clients their cash" (Field Interview, 2021).

The cost effect demonstrated that most banks have lost reputation and huge sum of money due to transaction issues, damaging their customer base. Furthermore, it was discovered that the banks were vulnerable because their secrets or codes and that of customers were exposed. Phishing and pharming are two types of cyber fraud that lead victims to believe they are dealing with the authorized institution not knowing they are being conned.

4.3.3 Why Cybercrime is still such a success in Banking

As long as cyber fraud exists, it is a booming business that provides the offenders with everything they require. This means that the majority of banks, and thus the victims, have systems that are vulnerable to fraudsters. Cybercrime or not, fraud is on the rise, according to the report, cybercrime is still a success thanks to the internet or computer network. And the fact that security is lax is one of the reasons why bank infiltration has become a simple chore for folks. According to the report, "most individuals are unaware of cyber fraud; thus, fraudsters continue to swindle most people with new tactics to gain whatever they want."

4.3.4 What entices fraudsters in banking?

This topic brought up the reality that cyber fraudsters are tempted by a variety of motives. The bulk of those who engage in this behaviour does so because they are jobless. According to one respondent, the practice has grown in popularity as a result of increased unemployment and the fact that it is most people's primary source of income. This suggests that individuals scamming

University of Education,Winneba http://ir.uew.edu.gh

banks through this strategy also utilized shoddy internal controls to examine their activities and problems.

"It's a successful endeavour because they make a lot of money that they'll never have made in a year," another interviewee stated. They are pushed to participate in illegal activities by a lack of employment, peer pressure, and the lavish lifestyle they see portrayed in the media.

4.4 How can Cybercrime threats be mitigated in the banking sector of Ghana?

With Ghana's growing Internet penetration, new online trade platforms have emerged, allowing the typical Ghanaian to perform a wide range of economic activities. Although the online portal facilitates the exchange of products and services, the vast majority of transactions take place offline. As a result, certain provisions of the Criminal Offences Act (29/30) have been reintroduced into the Electronic Transactions Act (Act 772) to make prosecuting cybercrime suspects easier. Among these are sections 20, 21, 23, 122, 124, 133, 137, and others. Crimes under these sections of the Criminal Offences Act 29/60, which have been reaffirmed in the Electronic Transactions Act (Act 772), are bailable offenses with a lighter penalty that does not discourage fraudsters.

4.4.1 Review Law on Cybercrime

The ratification of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and the Convention on Cybercrime (Budapest Convention) by Parliament in 2018 and 2019 requires Ghana to establish appropriate mechanisms for cybersecurity governance, to combat cybercrime, promote cybersecurity and facilitate both domestic and international cooperation in the fight against cybercrime. The implementation of the law is expected to enhance and reaffirm Ghana’s leadership on cybersecurity matters in the sub-region (Comunication-Ministry, 2020). Parliament of Ghana passed the bill Cybersecurity

University of Education,Winneba http://ir.uew.edu.gh

Act 2020, which promotes and regulates cybersecurity activities. The law established a regulatory body called Cyber Security Authority, to protects the critical information infrastructure of the country, regulates cybersecurity activities, provides the protection of children on the internet, and develops Ghana's cybersecurity ecosystem.

4.4.2 Strict Law enforcement

The Cyber Crime Unit is equipped with a state-of-the-art Digital Forensics Laboratory for digital forensics examination and a Cyber Patrol Section for advanced online monitoring and surveillance of Ghana's cyberspace for crime detection.

According to the Minister of Communication and Digitization, Mrs. Ursula Owusu-Ekuful, the Cyber Crime Unit's involvement is not limited to criminal acts commonly associated with technology itself—such as hacking—but extends to investigations of more traditional offenses such as fraud, threats, and other serious crimes where a digital device was the means used.

4.4.3 Education on Cybercrime

The creation of cybersecurity awareness in the country will go a long way to minimize the exploitation of vulnerable citizens. Seminars, workshops, and symposiums should be organized to educate the general public on the baits used by fraudsters in extorting money and other damages.

People should be made aware of frivolous offers or deals that look so genuine, and make background checks or consult before entering into any transaction with people or firms that may end up being scammers.

4.4.4 Cybersecurity measures

University of Education,Winneba http://ir.uew.edu.gh

The banks should deploy cybersecurity measures that will help protect online transactions by their customers. The website of banks must be secure and periodically enhance its security mechanisms to avoid vulnerabilities. However, penetration tests should be run often by the system administrators to detect possible vulnerabilities that may exist and find measures to curb them before hackers detect and use them to exploit and cause cash suppression and other forms of cyber fraud.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATION

5.1 Summary

The goal of the study was to evaluate bank cybercrime. However, the specific goals were to determine facets of cybercrime, investigate major threats that banks face in today's cybercrime, and determine ways to mitigate cybercrime in banks.

The study has yielded to its main purpose and all objective outline were carefully scrutinized to be satisfactory.

5.2 Findings of the Study

Based on the analysis of the study the following findings are made. The findings are about the various objectives studied; As regards the first objective which sought to identify the facets of cybercrime in Ghana, it was found that generally, the facets of cybercrime are: *Hacking, Phishing, Relationship fraud, Investment fraud, Account takeover, Identity theft, Credit card fraud, Money Laundering, Mobile money fraud and, online purchase fraud*.

These facets of cybercrime were common in our setting and many have fallen victims to one or more of their exploitations. As some victims narrate their ordeal, it reveals that they were made to believe it was genuine.

Concerning the second objective that investigated the major threats, it was found that most banks exploited, do run into bad debts. Their customers go through challenges and hence forsake their banks, and some cases blacklisting the banks. It was found that operating bank in this technological age is a challenge and risky because of cybercrime. Conclusively, Extortions,

University of Education,Winneba http://ir.uew.edu.gh

disclosure of bank secrets, weaknesses in the management of online transactions, and hacking have made banks vulnerable to exploitation.

In finding ways to control or mitigate the threats of cybercrime in banking, the third objective was met. It was found that to control the threats and vulnerability of banks from cybercrime perpetrators there must be a review of the cybercrime act, strict enforcement of the cybercrime act, education on the menace and acts of cyber fraud, and hardening of the management security systems. It was gathered that when the reviews are made on making the punishment of the cyber fraud act more severe, perpetrators may be extremely careful and desist from the act. However, when seminars and workshops as well as education symposiums are organized to educate the general public and the banks on the operations of the fraudsters, victims may be careful in entering into any transaction online. Investigating the background of individuals or organizations before transacting business with them must be a benchmark.

5.3 Conclusion

Banking, though relevant in managing the finances of customers yet its activities are sabotaged by cyber fraud. This business enterprise has become a crime mostly perpetrated by educated people who are believed to have various understandings of computer applications. Based on the findings it is conclusive that, cyber fraud has an immense negative impact on banking. Thus, the activities of cyber fraudsters like hacking, phishing, and others have been operated against banks. This crime has thrived for a long time because some insiders of banks have directly and indirectly supported this crime differently. Cybersecurity measures have been neglected by bankers hence cybercrimes have become open. This action has helped cyber fraudsters to perpetuate this canker with ease. Adopting public education and, the right banking measure and

University of Education,Winneba http://ir.uew.edu.gh

building better internet and cybersecurity systems have the propensity to avert tendencies of fraud.

5.3 Recommendation

The following recommendations are made based on the findings of the study;

Security Maintenance

Adequate security precautions should be taken. To avoid being hacked, banking institutions must implement strong cybersecurity measures. To protect against cybercrime, banks' websites must be well-protected. Penetration tests should be performed regularly to check for vulnerabilities in the bank's computer systems.

To protect customers who will conduct transactions online, additional security authentication should be implemented. This can be accomplished by implementing a one-time validation code that is sent to the customer whenever he or she attempts to login. The codes can be sent via SMS or email to the customer.

Monitoring of Banking Staff

Bank employees must be screened. Relevant information that makes up the bank's secrets must be well encrypted and kept safe from suspects on the inside. This will help to avoid situations in which insiders reveal secrets to outsiders. This method can be used to assess physical security. Furthermore, closed-circuit cameras can be installed at vantage points to monitor any suspicious activities in the baking hall.

University of Education,Winneba http://ir.uew.edu.gh

Adopt Advanced Management Technology

The management of banks must adopt proper technology to protect their business. This will help electronic transactions easily and formidable. Management policies on account privileges and credentials should be reviewed periodically to avoid staff login credentials being compromised.

Banking operation Laws

Adequate cyber laws must be enacted and applied. This effort will help the security agencies to probe suspicious activities found on the internet.

University of Education,Winneba http://ir.uew.edu.gh

REFERENCES

Abbatt, J. (1999). *Inventing the Internet. Cambridge,.* Cambridge: The MIT Press.

Abotchie, C. (2012). *Sociology of Urban Communities.* Accra: Hans Publication.

Adeniran, A. (2008). The Internet and Emergence of Yahooboys subCulture in Nigeria. *International Journal of Cyber Criminology*.

Aidoo, D., Akotoye, F., & Ayebi-Arthur, K. (2012). Locating computer crime in the use of ICT for management of educational system in Ghana-. *Academic 419":*, 102-111.

Ashok, I. (2016, October 27). *Hackers target all major UK banks with new Twitter phishing campaign*. Retrieved June 8, 2019, from International Business Times: https://www.ibtimes.co.uk/hackers-target-all-major-uk-banks-new-twitter-phishing-campaign-1588498

Association of Certified Fraud Examiners. (2004). *What Is Fraud?* Retrieved June 24, 2019, from Association of Certified Fraud Examiners: https://www.acfe.com/fraud-101.aspx

AVTEST IT Security Institute. (2019). *Malware*. Retrieved June 9, 2019, from AVTEST IT Security Institute: https://www.av-test.org/en/statistics/malware/

Bamrara, A. (2012). Journal of Internet Banking and Commerce. *An Explorative Study of Satisfaction Level of Cyber-crime*, 3.

Bocetta, S. (2018, November 16). *Advanced Phishing Kits now Available on the Dark Web*. Retrieved June 9, 2019, from GlobalSign Blog: https://www.globalsign.com/en/blog/warning-advanced-phishing-kits-now-available-on-the-dark-web/

BoG. (2021). *2020 BankingI Fraud Report.* Accra: Bank of Ghana.

Breach Level Index. (2018). *Request access to Data Breach Report*. Retrieved June 10, 2019, from Breach Level Index: https://www.breachlevelindex.com/request-report

Bryman, A. (2008). *Social Research Methods* (3 ed.). New York: Oxford University Press.

Burrell, B. M. (2008). Internet safety gone wild. *Sacrificing the educational and psychosocial benefits of online social environments*, 34 – 42.

University of Education,Winneba http://ir.uew.edu.gh

Castells, M. (2000). *The Rise of the Network Society,* (Vol. 1). Oxford: Blackwell Publishing Ltd.

CitiBusinessNews. (2021). *Strigent measures to minize fraud - Ghana Associaion of Bankers.* Accra: Ghana German economic Association (ggea.net).

Comunication-Ministry. (2020). *Cybersecurity Act* . Retrieved from moc.gov.gh: https://www.moc.gov.gh/cybersecurity-act-passed-promote-regulate-cybersecurity-activities

Corbin, J., & Strauss, A. (2008). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques* (3 ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2009). *Qualitative, Quantitative and Mixed Methods Approaches* (3 ed.). London: Sage Publications, Inc.

DiMarco, H. (2003). *The electronic cloak: Secret sexual deviance in cyber society.* Portland: Willan Publishing.

Edelman, B. (2009). Red Light States: Who Buys Online Adult Entertainment? *Journal of Economic perspectives*(23), 209-220.

Ennin, D. (2015). *CYBERCRIME IN GHANA: A STUDY OF OFFENDERS, VICTIMS AND THE LAW.* Accra: University of Ghana Space.

Financial Institutions and Cybercrime: Threats, Challenges and opportunities. (n.d.). Retrieved from RUSI: https://rusi.org/publication/newsbrief/financial-institutions-and-cybercrime-threats-challenges-and-opportunities

Flinders, K. (2016, January 29). *HSBC online services hit by DDoS attack*. Retrieved June 8, 2019, from ComputerWeekly: https://www.computerweekly.com/news/4500272109/HSBC-online-services-hit-by-DDoS-attack

Furnell, S. (2002:7). *Cybercrime: Vandalizing the Information Society.* London: Addison-Wesley.

Gartner. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*. Retrieved June 15, 2019, from Gartner:

University of Education,Winneba http://ir.uew.edu.gh

https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

GhanaPolice. (2017). *Cyber-crime.* Retrieved December 2, 2021, from police.gov.gh: https://police.gov.gh/en/index.php/cyber-crime/

GhanaWeb. (2013, August 1). *Cyber crime: Ghana 2nd in Africa, 7th in the world*. Retrieved June 23, 2019, from GhanaWeb: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Cyber-crime-Ghana-2nd-in-Africa-7th-in-the-world-281095

GhanaWeb. (2013, August 1). *Cyber crime: Ghana 2nd in Africa, 7th in the world*. Retrieved from GhanaWeb: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Cyber-crime-Ghana-2nd-in-Africa-7th-in-the-world-281095

GhanawebNews. (2021). *Arrested Internet fraudster also own cannabidol farm in Ashanti region.* Accra: Ghana Web portal.

Grant, C., & Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research:. *Creating the Blueprint for Your "House, 4*(2), 13.

Grant, C., & Osanloo, A. (2014). Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research:. *Creating the blue Blueprint for Your "House*, 13.

Graphic Online. (2014, February 21). *2 Prudential Bank officials in court for defrauding Singaporean bank of $611,649*. Retrieved June 22, 2019, from Graphic Online: https://www.graphic.com.gh/news/general-news/2-prudential-bank-officials-in-court-for-defrauding-singaporean-bank-of-611-649.html

Graphic Online. (2014, February 21). *Graphic Online*. Retrieved June 22, 2019, from 2 Prudential Bank officials in court for defrauding Singaporean bank of $611,649: https://www.graphic.com.gh/news/general-news/2-prudential-bank-officials-in-court-for-defrauding-singaporean-bank-of-611-649.html

Graphic Online. (2015, June 23). *Banks warned: Cheque fraud on the rise*. Retrieved June 22, 2019, from Graphic Online: https://www.graphic.com.gh/business/business-news/banks-warned-cheque-fraud-on-the-rise.html

University of Education,Winneba http://ir.uew.edu.gh

Graphic Online. (2015). *Cabinet to give nod to cybersecurity policy this month*. Retrieved June 9, 2019, from Graphic Online: https://www.graphic.com.gh/news/general-news/cabinet-to-give-nod-to-cybersecurity-policy-this-month.html

Graphic Online. (2015, May 20). *Commercial banks must help stop cheque fraud*. Retrieved June 22, 2019, from Graphic Online: https://www.graphic.com.gh/business/business-news/commercial-banks-must-help-stop-cheque-fraud.html

Graphic Online. (2015, March 24). *Kumasi: Man arrested for defrauding bank customers* . Retrieved June 22, 2019, from Graphic Online: https://www.graphic.com.gh/news/general-news/kumasi-man-arrested-for-defrauding-bank-customers-video.html

Graphic Online. (2016, May 30). *Graphic Online*. Retrieved June 22, 2019, from Bank fraudster arrested trying to dupe another customer: https://www.graphic.com.gh/news/general-news/bank-fraudster-arrested-trying-to-dupe-another-customer.html

Graphic Online. (2016, June 1). *Police grab alleged bank fraudster*. Retrieved June 22, 2019, from Graphic Online: https://www.graphic.com.gh/news/general-news/police-grab-alleged-bank-fraudster.html

Graphic Online. (2017). *UGBS partners cybersecurity company to educate students to combat threats of cyber fraud*. Retrieved November 21, 2019, from Graphic Online: https://www.graphic.com.gh/news/education/ugbs-partners-cybersecurity-company-to-educate-students-to-combat-threats-of-cyber-fraud.html

Graphic Online. (2018, September 6). *Ghana loses Gh¢30.1 million to bank fraud*. Retrieved June 22, 2019, from Graphic Online: https://www.graphic.com.gh/news/general-news/cyber-fraud-cases-on-the-rise-in-banking-industry-in-ghana-bog.html

Graphic Online. (2019). *Parliamentary Select Committee on Communications to train on cybersecurity*. Retrieved January 19, 2019, from Graphic Online: https://www.graphic.com.gh/news/general-news/parliamentary-select-committee-on-communications-to-train-on-cybersecurity.html

Hennink, M., Hutter, I., & Bailey, A. (2011). *Qualitative Research Methods.* Los Angeles: Sage Publications Inc.

Holt, T. J., & Blevins, K. R. (2007). Examining sex work from the client‟s perspectives. *Assessing johns using online data. Deviant Behavior*(28), 49-61.

University of Education,Winneba http://ir.uew.edu.gh

INTERPOL. (2021, 10 21). *INTERPOL report identifies top cyberthreats in Africa*. Retrieved from www.interpol.int: https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa

Jaikumar, V. (2007, March 29). *TJX data breach: At 45.6M card numbers, it's the biggest ever*. Retrieved from Computerworld: https://www.computerworld.com/article/2544306/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html

Kabay, E. (2008). *Computer Security Handbook,* (5 ed.). (W. Eric, Ed.) New York: John and Wiley.

Kumasi Metropolitan Assembly. (2019). *Brief of KMA*. Retrieved June 5, 2019, from Kumasi Metropolitan Assembly: http://www.kma.gov.gh/kma/?brief-on-kma&page=5143

Kumekpor, T. K. (2002). *Research Methods and Techniques of Social Research.* Accra: SonLife Press & Service.

Kwablah, E. (2009, February 17). Retrieved from https://www.ghanabusinessnews.com/2009/02/17/cyber-crime-giving-a-bad-name-to-ghana

Kwablah, E. (2009, February 17). *Cyber crime: Giving a bad name to Ghana*. Retrieved December 12, 2018, from Business and Financial Times: http://ghanabusinessnews.com/2009/02/17/cyber-crime-giving-a-bad-name-to-ghana

Ling, R. (2004). *The Cell Phone Impact on Society.* Elsevier: San Francisco,, United States of America.

Magele, T. (2005, February 16/17). *White Paper prepared for the*. Retrieved October 22, 2009, from E-security in South Africa: www.forgeahead.co.za/

Morse, J. (1991). Approaches to qualitative-quantitative methodological triangulation. *Nursing Research,*, 120-123.

MyjoyOnline. (2017, September 11). *MyjoyOnline*. Retrieved June 24, 2019, from MyjoyOnline: https://www.myjoyonline.com/business/2017/September-11th/new-capital-requirement-could-force-15-banks-to-go-down.php

National Cyber Security Centre. (2018). *"Legislation on cybersecurity will address weaknesses in our cybercrime laws* . Retrieved May 5, 2019, from National Cyber Security Centre:

University of Education,Winneba http://ir.uew.edu.gh

https://cybersecurity.gov.gh/index.php/legislation-on-cybersecurity-will-address-weaknesses-in-our-cybercrime-laws-ursula-owusu-ekuful/

National Cyber Security Centre. (2018). *Cybersecurity Fund to be Introduced in 2019 Budget*. Retrieved April 26, 2019, from National Cyber Security Centre: https://cybersecurity.gov.gh/index.php/cybersecurity-fund-to-be-introduced-in-2019-budget-finance-minister/

National Development Planning Commission. (2012). *Annual Progress Report.* Accra: National Development Planning Commission.

Neuman, L. W. (2003). *Social Research Methods: Qualitative and Quantitative Approached* (4 ed.). Boston: Pearson Education, Inc.

Olayemi, J. O. (2014). *Combating the Menace of Cybercrime, 3*(6), 980-991.

Olayemi, J. O. (2014). *International Journal of Sociology and Anthropology, 6*(3), 116-125.

Oxford English Dictionary. (2005). *Money laundering* (3rd ed ed.). UK: Oxford University Press.

Pati, P. (2003). *New Delhi*. Retrieved February 23, 2010, from Cybercrime: http://www.naavi.org/pati/pati_cybercrimes_dec03.htm

Privacy Rights Clearinghouse. (2015). *Data Breaches*. Retrieved June 9, 2019, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breaches

pwc Global. (2018). *Pulling fraud out of the shadows*. Retrieved June 8, 2019, from PwC's 2018 Global Economic Crime and Fraud Survey: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

Rollins, J., & Wyler, L. (2013). Retrieved from http://www.fas.org/spg/crs/terro/R41004.pdf

Rouse, M. (2017, October). *SearchSecurity*. Retrieved June 23, 2019, from Phishing: https://searchsecurity.techtarget.com/definition/phishing

RSA. (2018). *Current State of Cybercrime*. Retrieved June 9, 2019, from RSA: https://www.rsa.com/content/dam/premium/en/white-paper/2018-current-state-of-cybercrime.pdf

University of Education,Winneba http://ir.uew.edu.gh

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

Sanders, J. (2018, December 18). *Why cryptojacking will become an even larger problem in 2019*. Retrieved June 9, 2019, from TechRepublic: https://www.techrepublic.com/article/why-cryptojacking-will-become-an-even-larger-problem-in-2019/

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

Shannon, L. (2016, November 2016). *Tesco Bank hack*. Retrieved June 8, 2019, from This is MONEY: https://www.thisismoney.co.uk/money/saving/article-3930118/Tesco-Bank-hack-happened-protect-account.html

Snail, S. (2009). Snail, S. (2009).Cyber Crime In South Africa-Hacking, cracking, and other unlawful online Activities. *Journal of Information, Law & Technology (JILT)*, 2.

Snyder, F. (2001). *Sites of criminality and sites of governance".*

Stickings, A. (2016). Financial Institutions and Cybercrime: Threats, Challenges and Opportunities. *Cybercrime*, 1 - 3.

Strauss, A. L. (1987). *Qualitative Analysis for Social Scientist.* Cambridge: Cambridge University Press Suman, S., Srivastava, N.,.

Suman, S., Srivastava, N., & Pandit, R. (2014). Cyber Crimes and Phishing Attacks. *International Journal on Recent Innovation Trends in Computing and Communication,*, 334-337.

Tesco Bank. (2016, November 12). *Tesco Bank hack*. Retrieved June 8, 2019, from This is MONEY: https://www.thisismoney.co.uk/money/saving/article-3930118/Tesco-Bank-hack-happened-protect-account.html

The Banking Association South Africa. (n.d.). *CHEQUE FRAUD SCAMS*. Retrieved June 22, 2019, from The Banking Association South Africa: https://www.banking.org.za/consumer-information/bank-crime/cheque-fraud-scams

University of Education,Winneba http://ir.uew.edu.gh

The Encylopedia . (2018, June 15). *Credit Card Fraud*. Retrieved June 24, 2019, from The Encylopedia of world problems & Human potential: http://encyclopedia.uia.org/en/problem/136735

Toronto SUN. (2013, September 28). *Why do banks commit so much fraud?* Retrieved June 15, 2019, from Toronto SUN: https://torontosun.com/2013/09/28/why-do-banks-commit-so-much-fraud/wcm/6f172bd9-aa86-4f7b-bb75-b513c5e66cfb

Van Der Merwe, D. (2008). *Information and Communication Technology Law.* Durban: LexisNexis.

Verizon. (2019). *2019 Data Breach Investigations Report*. Retrieved June 9, 2019, from Verizon: https://enterprise.verizon.com/resources/reports/dbir/

Vijayan, J. (2007, March 29). *TJX data breach: At 45.6M card numbers, it's the biggest ever*. Retrieved June 24, 2019, from Computerworld: https://www.computerworld.com/article/2544306/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html

Vijayan, J. (2007, March 29). *TJX data breach: AT 45.6M card numbers, it's the biggest ever*. Retrieved from Computerworld: https://www.computerworld.com/article/2544306/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html

Warner, J. (2011). Understanding Cyber-Crime in Ghana. *A View from Below Understanding Cyber-Crime in Ghana*, 736–749.

Warner, J. (2011). Understanding Cybercrime: A View from Below. *International Journal of Cyber Criminology*, 736-749.

Weber, A. W. (2003). The Council of Europe‟s Convention on Cybercrime. *Berkeley Technology Law Journal*, 426-446.

Webroot. (2019). *When it comes to cybersecurity, the only thing constant is change*. Retrieved June 9, 2019, from Webroot: https://www-cdn.webroot.com/6715/2122/9225/2018-Threat-Report-Infographic-sm.pdf

Wikipedia. (2018, January 7). *Float*. Retrieved June 22, 2019, from Wikipedia: https://en.wikipedia.org/wiki/Float_(money_supply)

Wikipedia. (2019, June 9). *Adobe Inc.* Retrieved June 24, 2019, from Wikipedia: http://edshare.soton.ac.uk/3222/2/_edshare_main.html

University of Education,Winneba http://ir.uew.edu.gh

Wikipedia. (2019, June 9). *Adobe Inc.* Retrieved from Wikipedia: http://edshare.soton.ac.uk/3222/2/_edshare_main.html

Wikipedia. (2019, April 30). *Cheque Fraud*. Retrieved June 22, 2019, from Wikipedia: https://en.wikipedia.org/wiki/Cheque_fraud

Wire Fraud. (2020). Retrieved from FindLaw: https://criminal.findlaw.com/criminal-charges/wire-fraud.html

World Bank. (2012). *ICT Competitiveness in Africa*. Retrieved January 10, 2019, from World Bank: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/282822-1346223280837/ICTCompetitiveness.pdf

Yar, M. (2013). *Cybercrime and Society* (2 ed.). London: Sage Publication,.

University of Education,Winneba http://ir.uew.edu.gh

APPENDIX I

Guided Questions used for the Interview

Ghana Police Service

1. How old are you?
2. What unit of the CID do you belong to?
3. What is your rank?
4. Have you been a victim of cyber fraud before?
5. Have you witnessed a cyber fraud case before?
6. Mention the types of cybercrime you know?
7. Has your unit received any report of cybercrime against an individual?
8. Has your unit received any complaints about cybercrime from the banks?
9. If yes, can you narrate any cybercrime incidence you have heard of or witnessed?
10. Mention at least two threats of cybercrime?
11. How do you think cybercrime can be controlled?
12. Which of the following measures do you think is appropriate to mitigate cybercrime?

University of Education,Winneba http://ir.uew.edu.gh

APPENDIX II

Guided Interview Questions for Bank Staff

1. How old are you?
2. Which bank do you work with?
3. What is your position at the bank?
4. Have you been a victim of cyber fraud before?
5. Have you witnessed a cyber fraud case before?
6. Mention the types of cybercrime you know?
7. Has your unit received any report of cybercrime against an individual?
8. Has your unit received any complaints about cybercrime in your bank banks?
9. If yes, can you narrate any cybercrime incidence you have heard of or witnessed?
10. Mention at least two threats of cybercrime?
11. How do you think cybercrime can be controlled?
12. Which of the following measures do you think is appropriate to mitigate cybercrime?

University of Education,Winneba http://ir.uew.edu.gh

APPENDIX III

Guided Interview Questions for CBD

1. How old are you?
2. Are you employed?
3. Where do you work?
4. What is your position do you occupy?
5. Have you been a victim of cyber fraud before?
6. Have you witnessed a cyber fraud case before?
7. Mention the types of cybercrime you know?
8. Has your unit received any complaints about cybercrime from the banks?
9. If yes, can you narrate any cybercrime incidence you have heard of or witnessed?
10. Mention at least two threats of cybercrime?
11. How do you think cybercrime can be controlled?
12. Which of the following measures do you think is appropriate to mitigate cybercrime?

University of Education,Winneba http://ir.uew.edu.gh

APPENDIX IV

Transcribe data from the interview

BANK PROCESSED DATA FROM INTERVIEW

```
FREQUENCIES VARIABLES=Age Gender Position Bank Years
  /STATISTICS=STDDEV MEAN MODE
  /PIECHART FREQ
  /ORDER=ANALYSIS.
```

Frequencies

Notes

Output Created		21-NOV-2021 16:07:17
Comments		
Input	Data	C:\Users\Miishee\Documents\BankQuestinnaire .sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	12
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.

University of Education,Winneba http://ir.uew.edu.gh

Syntax		FREQUENCIES VARIABLES=Age Gender Position Bank Years /STATISTICS=STDDEV MEAN MODE /PIECHART FREQ /ORDER=ANALYSIS.
Resources	Processor Time	00:00:08.22
	Elapsed Time	00:00:07.17

[DataSet1] C:\Users\Miishee\Documents\BankQuestinnaire .sav

Statistics

		Age of Respondent	Gender	Position	Bank	Years of Service
N	Valid	12	12	12	12	12
	Missing	0	0	0	0	0
Mean		37.75	1.5000	3.8333	8.0833	11.92
Mode		35	1.00[a]	3.00[a]	7.00	6[a]
Std. Deviation		7.436	.52223	1.74946	5.99179	7.645

University of Education,Winneba http://ir.uew.edu.gh

a. Multiple modes exist. The smallest value is shown

Frequency Table

Age of Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	29	1	8.3	8.3	8.3
	30	1	8.3	8.3	16.7
	31	1	8.3	8.3	25.0
	32	1	8.3	8.3	33.3
	35	3	25.0	25.0	58.3
	40	1	8.3	8.3	66.7
	42	1	8.3	8.3	75.0
	44	1	8.3	8.3	83.3
	48	1	8.3	8.3	91.7
	52	1	8.3	8.3	100.0
	Total	12	100.0	100.0	

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	6	50.0	50.0	50.0
	Female	6	50.0	50.0	100.0
	Total	12	100.0	100.0	

University of Education,Winneba http://ir.uew.edu.gh

Position

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Branch Manager	1	8.3	8.3	8.3
	Accountant	2	16.7	16.7	25.0
	Relation Manager	3	25.0	25.0	50.0
	Credit Officer	1	8.3	8.3	58.3
	Investment Officer	2	16.7	16.7	75.0
	Banker	3	25.0	25.0	100.0
	Total	12	100.0	100.0	

Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Access Bank	1	8.3	8.3	8.3
	ADB	1	8.3	8.3	16.7
	ABSA	1	8.3	8.3	25.0
	CBG	1	8.3	8.3	33.3
	First Atlantic	1	8.3	8.3	41.7
	ECOBANK	2	16.7	16.7	58.3
	FIDELITY	1	8.3	8.3	66.7
	GCB	1	8.3	8.3	75.0
	GT BANK	1	8.3	8.3	83.3
	APEX BANK	1	8.3	8.3	91.7
	Bank of Ghana	1	8.3	8.3	100.0
	Total	12	100.0	100.0	

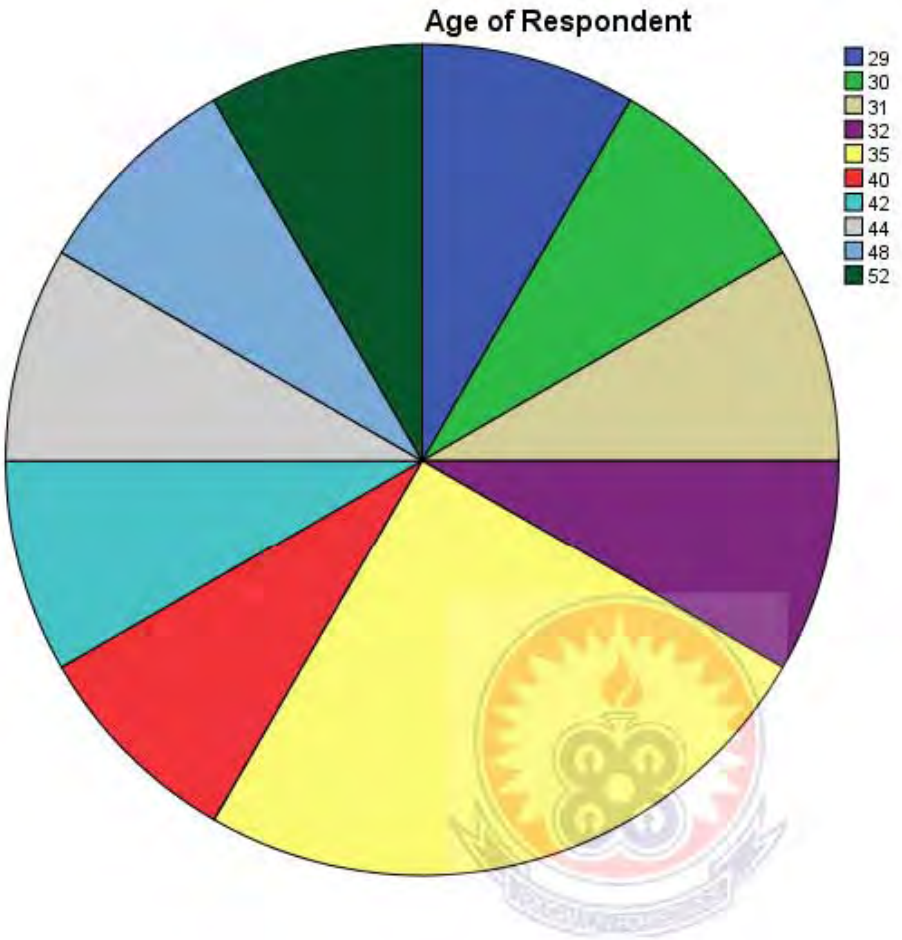
University of Education,Winneba http://ir.uew.edu.gh

Years of Service

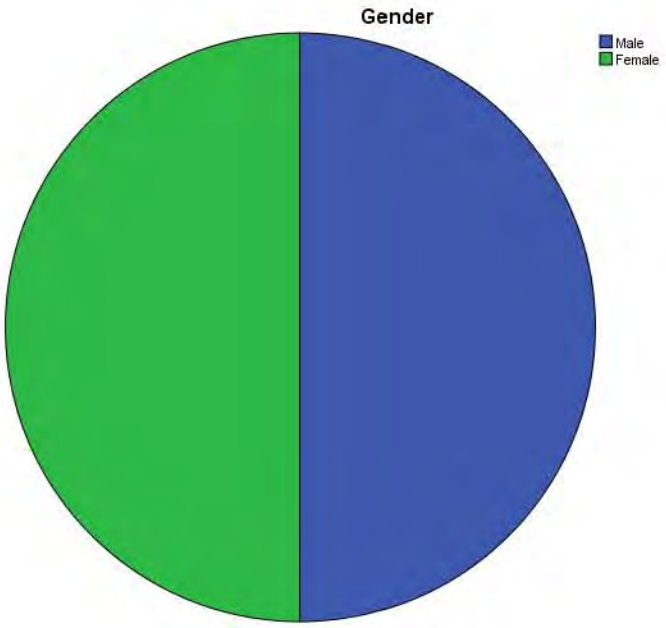
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	8.3	8.3	8.3
	4	1	8.3	8.3	16.7
	6	2	16.7	16.7	33.3
	8	2	16.7	16.7	50.0
	9	1	8.3	8.3	58.3
	16	2	16.7	16.7	75.0
	18	1	8.3	8.3	83.3
	23	1	8.3	8.3	91.7
	26	1	8.3	8.3	100.0
	Total	12	100.0	100.0	

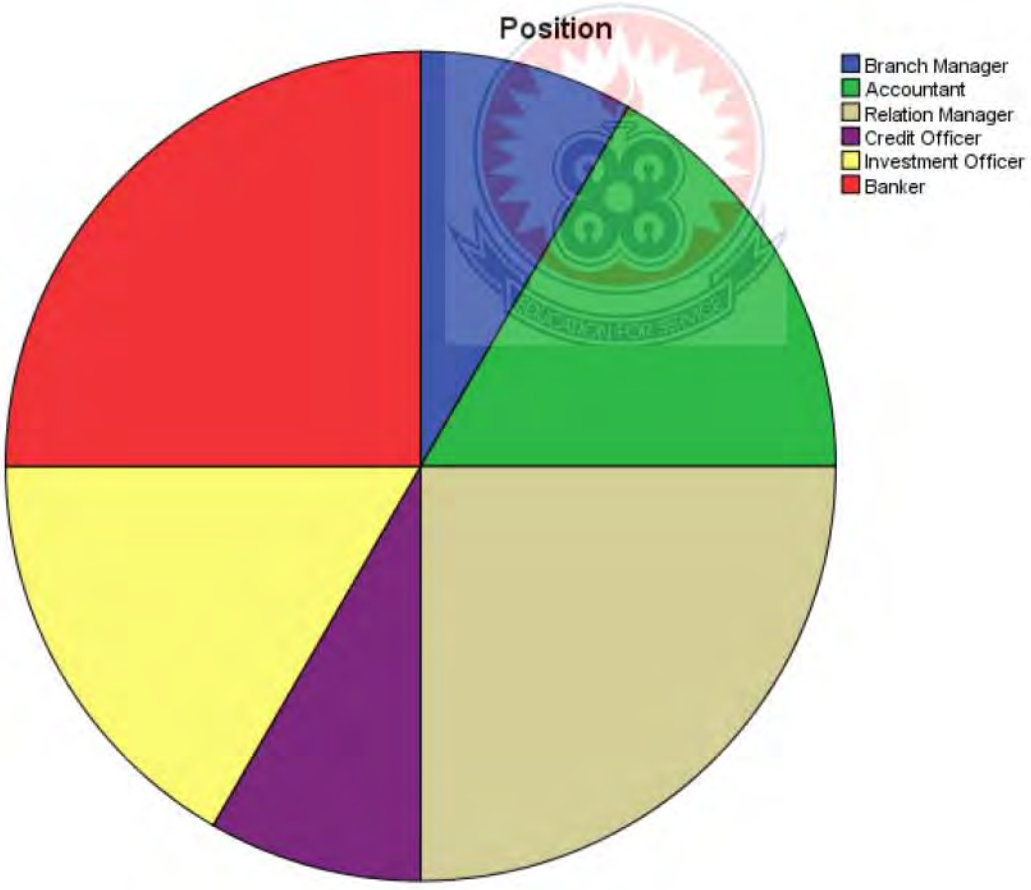
University of Education,Winneba http://ir.uew.edu.gh

Pie Chart

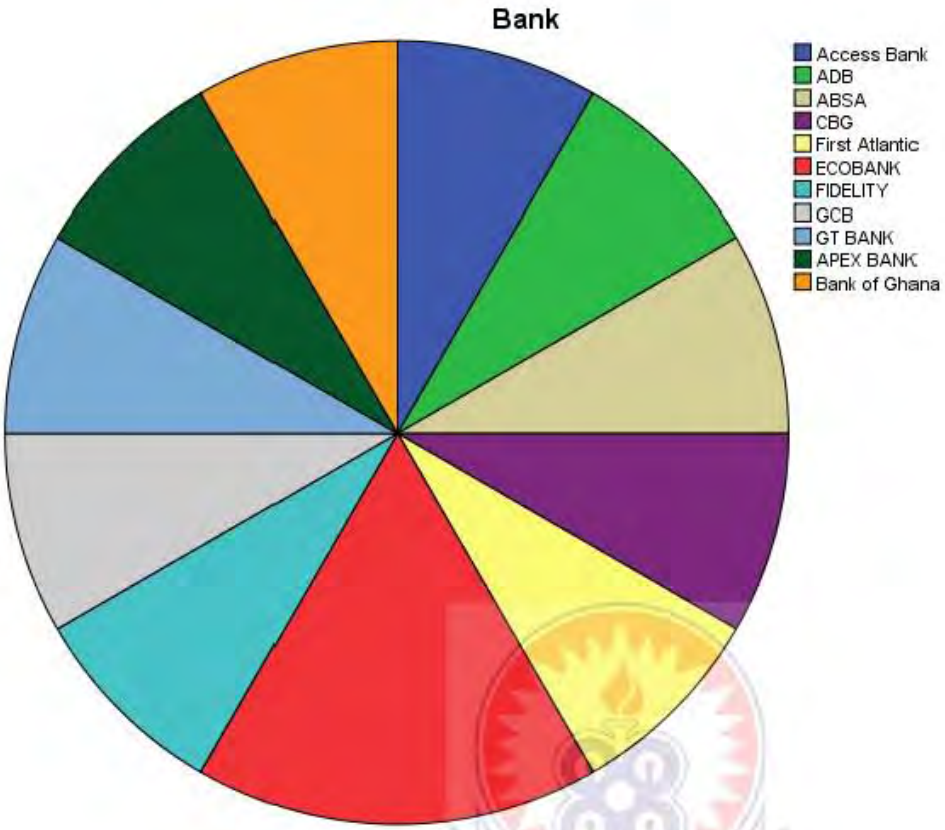


University of Education,Winneba http://ir.uew.edu.gh





University of Education,Winneba http://ir.uew.edu.gh



University of Education,Winneba http://ir.uew.edu.gh