THE EVALUATION OF CYBERCRIME ASSOCIATED WITH THE E-BANKING IN NIGERIA.

BY

LEGUNSEN OLAYINKA OLUWASEUN
17012411001
CSC/CHEM

A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, TAI SOLARIN COLLEGE OF EDUCATION, OMU – IJEBU, OGUN STATE, NIGERIA

IN PARTIAL FULFILMENT FOR THE REQUIREMENT OF NIGERIA CERTIFICATE IN EDUCATION (N.C.E)
MARCH, 2020.

CERTIFICATION

This is to certify that this project work titled "The Evaluation Of Cybercrime Associated With The E-Banking in Nigeria" was carried out by **Legunsen Olayinka Oluwaseun,** Matric. No: 17012411001 in the Department of Computer Science, Tai Solarin College of Education, Omu-Ijebu under my supervision.

---------- ----------

Mrs. Adu D.O **Date**
(Supervisor)

DEDICATION

This research project is dedicated to Almighty God, my creator, source of inspiration, wisdom, knowledge and understanding. He has been the source of my strength throughout this programme.

ACKNOWLEDGEMENT

My sincere gratitude goes to almighty God for His favour and protection throughout this research work and my stay in the college.

I acknowledge the effort of my supervisor, Mrs. Adu D.O in going through this project with patience, criticisms and suggestions which resulted in the success of this research work

Sincere, I express my gratitude to my Head of Department, in Person of Mr. O.A Johnson and other lecturers in the department for being there for me.

I also express my profound gratitude to my dear parents Mr. and Mrs. Legunsen Ojikutu for their moral, financial assistance and encouragement because without their mutual understanding this brain would not have come to existence.

It is highly necessary to acknowledge my source into the world, my most loving and caring mother Mrs. Legunsen for her support spiritually, morally, financially and academically, I pray you eat the fruit of your labor.

My heart appreciate also goes to my blood sister Miss Oluwaseun Legunsen and a brother like father Mr. Legunsen Olusola for their support towards the success of this programme.

My sincere love and appreciation also goes to my school mother like no other Miss Senkoya Oluwaseyi for the love and care, I will miss you so much momma.

My appreciation goes to my hostel mates and my school daughter (Ayodele Taiwo) who has always been there when their help is needed. I am also expressing my sincere gratitude to everyone who had contributed to the successful completion of my study either financially, materially, spiritually and morally.

My acknowledgement will not be complete without my siblings, sincere appreciation goes to my dearest siblings: Arthur Victor Legunsen, Arthur Mojoyinola Legunsen and Arthur Ayinke Legunsen (Rest on sister, I will forever miss you).

My sincere thanks goes to all my colleagues (Elegbede Daniel, Dayo Temidire Thomas, Ajayi Opeyemi, Sanya Adesola,) and my special advisers Tajudeen Abibat, Afolabi Olayinka Precious in Tai Solarin College of education.

Finally, my sincere thanks and appreciation goes to others whose names are not mentioned in this work. May God bless you all (Amen).

TABLE OF CONTENTS

ABSTRACT

The study evaluates cybercrimes associated with e-banking. The objectives of the study include identifying various cybercrimes associated with e-banking, identifying cause/motives of e-banking cybercrimes, determining perceived effects of e-banking cybercrimes and to determine the solutions to the problems of cybercrimes that are related to e-banking in Ogun State.

Concerning methodology for this study, data was obtained from primary source that is questionnaire and secondary source which include text books and journals. The respondents for the study comprised of workers and students. A total of 100 respondents were randomly selected for the study. Hence, questionnaire was distributed to capture responses from the respondents. The quantitative data were analysed using IBM SPSS version 23.

The study has the following findings; there are various cybercrime associated with e-banking, they are cause/motives militating against effective e-banking services, they are the perceived effects of e-banking cybercrimes, they are the solutions to the problems of cybercrimes that are related to e-banking and there is a significant relationship between e-banking and cybercrime. This research serves as contribution to the body of literature in the area of the effect of personality trait on student‟s academic performance, thereby constituting the empirical literature for future research in the subject area.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

There are few innovations that have changed the dynamics of banking as much as the e-banking revolution. Throughout the world, banks are reorganizing their business strategies to take advantage of new business opportunities offered by e-banking. Electronic banking is believed to have started in the early 1980s (Shandilya, 2011). It has since then been growing in an unprecedented dimension in line with the growth in ICT development. E-banking has enabled banks to overcome borders, adopt strategic outlook, and bring in new possibilities. According to Nitsure (2010), information communication technology has reduced the cost of processing and facilitating the transmission of information leading to drastic changes in the banking business. It is worth noting that e-banking has not been limited to advanced countries, but is found even in countries with underdeveloped e-banking systems, as a result of the many new business opportunities offered by e-banking.

Although no official definition of e-banking has been established, it generally implies a service that allows customers to use some form of computer to access account-specific information and possibly conduct transactions from a remote location like home or workplace. Additionally, e-banking has obvious advantages to the customer in terms of convenience where customers conduct routine banking transactions from the comfort and security of any location from which they wish to transact. The emerging concept of e-banking has drawn the attention of the business fraternity as well as of scholars and researchers to the effects of such dynamics on the banking industry. For instance, Liao

and Wong (2008) in their study of the determinants of customer interactions with Internet-enabled e-banking found that factors such as perceived usefulness, ease of use, security, convenience, and responsiveness to service requests to be a strong measure of the variation in customer interactions. Based on this finding, they suggested that stringent security control is critical to e-banking operations. Such arguments do not only have managerial implications for enhancing Internet banking operations and developing viable electronic banking services, but also form the basis upon which this study is based.

E-banking technology created a revolution by extending banking hours beyond office hours and beyond national boundaries (Balachandran and Balachandher, 2011). In Nigeria, several studies on e-banking have been done. Chiemeke, et. al. (2012), for instance, conducted a pragmatic study on adoption of e-banking where major hindering factors to Internet banking adoption such as insecurity and inadequate operational facilities, including telecommunications facilities and electricity supply, were identified.

Crime and corruption represent a major concern for business executives not only in Nigeria but also in other parts of Africa (Olasanmi, 2013). In Nigeria, for instance, the most serious impediments to economic activities and business are crime and corruption which averages 75% and 71% respectively. Theft and fraud are the second most popular crimes after burglary. By definition, cybercrime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cybercrime is believed to have started in the 1960"s in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of

illegal materials in the 1970s. The 1980s witnessed the introduction of viruses. The fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space. Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes. With e-banking gaining ground in Nigeria and other parts of sub-Saharan Africa, customers and online buyers are facing great risk of unknowingly passing on their information to fraudsters. "Hackers" get information of those who have made purchases through websites and then make fake cards, which they use with less detection. Absence of a law specifically dealing with card-related crimes in Nigeria may be giving thieves a loophole to operate freely (Olasanmi, 2013). Police treat card-related crimes like any other case of fraud.

1.2 Statement of the Problem

This study would examining the types of cybercrimes that have economic impact either directly or indirectly on the financial system of a nation or having cross border ripple effects with focus on e-banking. Longe and Chiemeke (2011) simplified the list of unintended consequences of ICT to include acts such as Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy -cat websites. While some types of cybercrimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries.

1.3 Objectives of the Study

The following are the objectives of the study:

1. To identify various cybercrimes associated with e-banking in Ogun State.

2. To identify cause/motives of e-banking cybercrimes in Ogun State.
3. To determine perceived effects of e-banking cybercrimes.
4. To determine the solutions to the problems of cybercrimes which are related to e-banking.

1.4 Research Questions

1. What are the various cybercrime associated with e-banking in Ogun State?
2. What are cause/motives militating against effective e-banking services in Ogun State?
3. What are the perceived effects of e-banking cybercrimes?
4. What are the solutions to the problems of cybercrimes that are related to e-banking?

1.5 Scope of the Study

This study would cover the cybercrime associated with e-banking in Nigeria using only Fidelity Bank Plc customers.

1.6 Significance of the Study

The outcome of this study would educate the general public especially the users of e-banking services on the relationship between e-banking and cybercrime. Also, this research would be a contribution to the body of literature in the area of the effect of personality trait on student‟s academic performance, thereby constituting the empirical literature for future research in the subject area.

1.7 Limitation of Study

Financial constraint- Insufficient fund tends to impede the coverage of the researcher in sourcing for the relevant materials, literature or information and in the process of data collection (internet, questionnaire and interview). Time constraint- The researcher will simultaneously engage in this study with other academic work. This consequently will cut down on the time devoted for the research work. Hence, the study is limited to the bank customers in Ijebu-Ode axis of Ogun State.

1.8 Definition of Terms

Cybercrimes: **Cybercrime** refers to crimes carried out using computers or the internet

e-Banking: A method of banking in which the customer conducts transactions electronically via the Internet.

Phishing: the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Cyber Terrorism: The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.

Spam Mails: Is unsolicited messages sent in bulk by email (spamming).

Cyber-Stalking: The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

There are few innovations that have changed the dynamics of banking as much as the e-banking revolution. Throughout the world, banks are reorganizing their business strategies to take advantage of new business opportunities offered by e-banking. Electronic banking is believed to have started in the early 1980s (Shandilya, 2011). It has since then been growing in an unprecedented dimension in line with the growth in ICT development. E-banking has enabled banks to overcome borders, adopt strategic outlook, and bring in new possibilities. According to Nitsure (2010), information communication technology has reduced the cost of processing and facilitating the transmission of information leading to drastic changes in the banking business. It is worth noting that e-banking has not been limited to advanced countries, but is found even in countries with underdeveloped e-banking system, as a result of the many new business opportunities offered by e-banking. The emerging concept of e-banking has drawn the attention of crimes. This chapter shall review related theories and concepts of e-banking and cyber-crime.

2.2 Theoretical Framework

This section discusses some theories relating to the electronic media and security issues. Electronic media have been emphasized by various theoretical traditions. Sociologists, for instance, argued that point-to-point communication mediator instance, telephones- support shared aims which demonstrate a powerful collective representation. Some, especially the Marxists, look at

communication media as an exploitative tool by the elitist groups for socioeconomic and political control in their own contribution to the digital communication. Bell, *et al,* (2009) argued that the invention of mini-electronic and optical circuits capable of speeding the rate of information flow through networks would have a big impact on society. Despite the positive impact of technology on society, it has on the other hand led to the unintended use in criminal activities like cybercrime. He concluded by saying, it is easier to steal a penny from millions of bank account owners using the internet than using physical robbery.

2.2.1 Routine Activity Theory

This theory proposes that three situations facilitate the occurrence of crime. Proponents argue that such events must happen at the same time and in the same space. The three situations are the existence of a suitable target, lack of security, and a motivated offender for the crime to occur (Jaishankar, 2008). The assessment of the situation determines whether or not a crime takes place.

2.2.2 Opportunity Theory

This theory does not focus on the events that contribute to the crime but on the opportunities that emerge as a result of preventive measures to curb the crime. Proponents of this theory argue that crimes transverse between location, time, target, direction, and method of committing the crime (Felson & Clarke, 2009). They further assert that Opportunity to commit a crime is a root cause of crime. Also, they posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in all crimes, not just those involving physical property thereby reducing opportunity of crime.

2.2.3 Technology Theory

The response of technology to the cyber-crime problems centre on the use of computer security theories to design and evolve solutions that provides authentication, verification, non-repudiation and validation. These theories and models rely on the use of cryptography, steganography, network protocols, and the use of software engineering process/models to develop systems that offer some form of protection for users and the information infrastructure. Cybercrime thrives on the web today because the internet did not inculcate in its protocols from the onset a mechanism that allows a host to selectively refuse messages. This implication is that a benign host that desires to receive some particular messages must read all messages addressed to it. In essence, a malfunctioning or malicious host has the capacity to send many unwanted messages (Crocker, 2011)). This problem is exacerbated by the ubiquitous nature of the web and remains the Achilles heel of the issue of web security today. Although all the theories discussed above are related to cyber-crime, we are inclined to adapt routine activity theory to this study because the theory captured the philosophical assumptions upon which this study is based.

2.2.4 Social Theories

From a social scientific point of view, security theories on providing and implementing protection against breaches and information system misuse have evolved. They focus on user security awareness, motivation, deterrents, technology and training (Proctor & Byrnes, 2012). Researchers have theorized that user perception of risks and choices based on those perceptions can influence

system security. The situational characteristics theory proponents argued that situations within a system usage domain can impact on ethics and user behaviour (Martins & Eloff, 2012).

Wood (2010) proposed the Human Firewall theory stating that those user actions can undo technical security measures. He advocated that organizations must sensitize and educate users and evaluate their compliance with security policies and procedures. The theory of least possible privilege as proposed by Beatson (2011) suggests psychological profiling of potential new users, while Bray (2002) argues that new users are more vulnerable to security breaches when using information systems (IS). Denning (2009) theorizes about defensive information warfare and proposes that security policy training and awareness will better equip users against threats. Kabay (2012) theorized about using social psychology as a tool to improve user security conduct. The importance of the interest of senior management and integrating security issues as part of the corporate asset protection model was highlighted by Katsikas (2010), Kovacich and Halibozek (2013). Vroom and Von Solms (2012) also modelled an Information System security awareness program to address end-users, IT personnel and management executives.

Sasse, *et al,* (2011) theorized that the nature of the technology with respect to the user‟s goals and intentions significantly influence security features and usage in IS systems. They went further to propose the use of training, punishment, and reporting security as a motivation for creating security awareness among users. Schlienger and Teufel (2012) adopted a socio cultural approach to information security and posited that the cultural theory can be used to enhance security at different cultural layers-namely, corporate policies, top management, and individuals. Siponen (2010) used

human morality as a force that can impact on security. Tudor (2011) argued for a theory that uses a holistic IS security architecture to incorporate infrastructure, policies, standards, awareness and compliance. He however, concentrated on awareness training at the expense of all the other components.

2.2.5 The Peel Theory

The Peel theory of community policing as highlighted by Longe *et al* (2010) assumes that violators or criminals and victims are usually proximate and used spatial distribution as a basis for apprehending criminals and solving crimes. This theory subsumes the role of the citizens in responding to partial and completed crime, crime control, and internal order and makes the police responsible for all crime control and law enforcement activities. Although some consensus exists among nations on how to combat and deal with crimes across borders using international policing such as the Interpol, the underlying theory still relates to the Peel model and it is therefore inadequate to face the cyber-crime problem. We cannot say as a matter of fact that there is any theory in existence from the criminal justice and policing angle that specifically addresses the problem of cyber-crime.

2.2.6 Space Transition Theory

Proponents of space transition theory argue that behavior of people in cyber space tends to bring out their compliance and noncompliance behavior both in the physical and in cyber space. This theory does not explain physical crime but cyber-crime and how people move and behave from one space to the other (Jaishankar, 2010). This entails persons with repressed criminal behavior (in the

physical space) having a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space, due to their status and position. It also implies that the status of persons in physical space does not transit to cyber space. Jaishankar (2010), for instance, argues that the individual behavior repressed in physical space is not repressed in cyber space.

2.3 E-Banking Crimes

Crime and corruption represent a major concern for business executives not only in Nigeria but also in other parts of Africa. In Nigeria, for instance, the most serious impediments to economic activities and business are crime and corruption which averages 75% and 71% respectively. Theft and fraud are the second most popular crimes after burglary (EFCC/NBS, 2010). By definition, cyber-crime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cyber-crime is believed to have started in the 1960‟s in the form of hacking.

This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s. The 1980s witnessed the introduction of viruses (Olasanmi, 2013). The fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space. Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes. With e-banking gaining ground in Nigeria and other parts of SSA, customers and online buyers are facing great risk of unknowingly passing on their information to fraudsters. "Hackers" get information of those who have made purchases through websites and then make fake cards, which they use with less detection. Absence of a law specifically dealing with card-related 11

crimes in Nigeria may be giving thieves a loophole to operate freely. Police treat card-related crimes like any other case of fraud.

2.4 Types of Cybercrime

This study presents the types of cyber-crimes that have economic impact either directly or indirectly on the financial system of a nation or having cross border ripple effects. Longe & Chiemeke (2011) simplified the list of unintended consequences of ICT to include acts such as Phishing, cyber terrorism, electronic spam mails, cyber-stalking, and fake copy -cat websites. While some types of cyber-crimes are specific to Nigeria, other types, such as identity theft and false statements, cut across all countries.

2.4.1 Phishing

According to Roger (2010) phishing is simply a high-tech identity theft that does not only steal personal information and identity from unsuspecting consumers, but also an act of fraud against the legitimate businesses and financial institutions that are victimized by phishing. Phishing is usually a social engineering crime pervasive in attacking organisations‟ or individuals‟ (customers‟) information systems (IS) in order to gather private information to be used against organisations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts (Rodger, 2010). According to recent estimates from the Anti-Phishing Working group (APWG, 2008) phishing scams remain a relatively small percentage of spam sent worldwide today. Phishing attempts to pose significant dangers for unsuspecting victims. It has become one of the fastest-growing worldwide threats on the Internet. This rapid growth has made combating it a huge priority

for electronic mail service providers, since phishing impacts every aspect of the Internet and computing and there is no single action from any one company or organization to solve the problem. The remedy can only come in a holistic fashion involving collaboration between technology innovation, industry, government, and user education as prescriptive guidance.

To build systems shielding users from fraudulent websites, designers need to know which attack strategies work and why. What makes a web site credible? This question has been addressed extensively by researchers in computer-human interaction. Successful phishing must not only present a high credibility web presence to its victims; it must create a presence that is so impressive that it causes the victim to fail to recognize security measures installed in web browsers (Rachna, *et al,* 2013) Data suggest that some phishing attacks have convinced up to 5% of their recipients to provide sensitive information to spoofed websites (Loftness, 2015). About two million users gave information to spoofed websites resulting in direct losses of $1.2 billion for U.S. banks and card issuers in 2003 (Litan, 2014).

If we hope to design web browsers, websites, and other tools to shield users from such attacks, we need to understand which attack strategies are successful and what proportion of users they fool. In an analysis of phishing attacks carried out in Rachna, *et, al,* 2013, found that good phishing websites fooled 90% of participants. Existing anti-phishing browsing clues are ineffective and 23% of participants in the study did not look at the address bar, status bar, or the security indicators.

Perpetrators target both document categories to secure personal identifying information. Often they obtain a „set" of point of information documents in order to present themselves as „legitimate 13

customers‟ to deceive the target organisation‟s authentication and verification processes to commit identity fraud (Kochems, 2013). Increasingly, the mode of attack for the fraud, especially the identity fraud perpetrator, is tending to rely on electronic commerce or mechanical/digital devices to initiate the identity theft or identity deception act. This is to some extent enabled by Internet adoption. For example, 77% of United States (US) adults were online in May 2006, up from 74% in 2005, 66% in 2002, 64% in 2001, and 57% in 2000, according to e-Marketer (2013). In phishing e-mail messages, the senders must gain the trust of the recipients to convince them to divulge their personal information. To gain this trust, fraudsters "spoof," or mimic, a reputable company. The companies spoofed most often are financial services- Internet organizations such as the Bank of America, Citibank, eBay, PayPal, etc. Retailers and Internet service providers are also targeted (APWG , 2008 & Litan, 2014).

These phishing e-mails are usually mass mailed, many of the recipients are not customers of the spoofed companies and may quickly realize that the e-mail is fraudulent, or may believe that the e-mail was mistakenly sent to them and ignore the e-mail. Fraudsters rely on the responses from the few recipients who are customers of the spoofed company and who fall victim to the scam. According to Longe, *et. al.* (2010) the scammers claim to be from reputable companies and go to great lengths to emulate the company‟s visible branding.

Their fraudulent e-mails often contain the company‟s logo and use similar fonts and color schemes as those used on the company‟s web site. Some of the fraudulent e-mails simply reference images from the legitimate company‟s site. The main link in a fraudulent e-mail sends the recipient to the

fraudulent phishing web site, but many fraudulent e-mails include other links that send the recipient to sections of the real company‟s web site.

To further convince the recipient that the e-mail originated from the reputable company, the scammers use a "from" e-mail address that appears to be from the company by using the company‟s domain name (e.g., @ebay.com, @paypal.com) (Longe, *et al*, 2010) Phishing e-mails also try to assure the recipient that the transaction is secure in hopes of gaining the recipient‟s trust. The following are assurances that were included in fraudulent e-mails: "Remember: eBay will not ask you for sensitive personal information (such as your password, credit card, bank account numbers, social security number, etc.) in an e-mail."

This e-mail then sends users to a fraudulent web site that asks for personal and account information while promising that the information is submitted via a secure server. The phishing perpetrators could then notify the victim of a "security threat." Such a message may be welcomed or expected by the victim, who would then be easily induced into disclosing personal information (Gaunt, 2011). The number of unique phishing websites detected by APWG during the second half of 2008 saw a constant increase from July to October with a high of 27,739 (APWG, 2008).

In Nigeria, the most recent phishing attacks were on the customers of Inter-switch, which remains the organization with the highest customer base in electronic transactions. The Nigeria Deposit Insurance Corporation (NDIC) disclosed in its 2007 annual report and statement of account that underhand deals by bank staff, among others, resulted in attempted fraud cases totalling over N10.01

billion (over 65 million USD) and actual losses of N2.76 billion (13 million USD) in 2007

With the present situation in the world economy and the appropriate technology, fraudulent action is most likely to increase and phishing remains one of the main means of performing "fraud without borders." The extent of readiness to stem phishing in Nigeria needs to be determined because fraudulent activities emanating from these nations have far-reaching consequences beyond her borders.

2.4.2 Vishing

Vishing is the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward. Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

The term "Vishing" is derived from a combination of "voice" and "Phishing (Ollmann, 2007). Vishing capitalizes on a person's confidence in the telephone service, as the target is usually not aware of scammer‟s ability to use techniques such as caller ID spoofing and advanced automated systems to commit this kind of scam (RSA, 2009). However, as the yield on traditional Phishing attacks continues to reduce, scammers have resorted to Vishing in an effort to acquire user's financial account numbers, passwords and other personal data. Years ago, children could just call an unknown landline and play a prank on them. However, even with circuit switching, digital and/or electromechanical, technologies, the call could be traced back to the telephone bill-payer once the

prank was reported to the Telco. But with the recent advancement in the IP telephony system, it means that there is a possibility that a telephone call could originate and/or terminate at a computer anywhere in the world. Besides, the amount to be paid is also negligible, thus making it more likely to engage in vishing scams.

Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Fraudsters also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on "social engineering" techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to assume your identity and open new accounts.

To avoid being fooled by a vishing attempt:

- If you receive an email or phone call requesting you call them and you suspect it might be a fraudulent request, look up the organization‟s customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate.

Though vishing and its relative, phishing, are troublesome crimes and sometimes hard to identify, here are some tips from the FTC to protect your identity.

2.4.3 Smishing

Here, we take a look at Smishing which is a form of Phishing that uses short messaging services (SMS) or text messages on mobile phones and Smartphone‟s (IC3/FBI, 2010). Smishing derived its name from the test messaging technology SMS (Short Message Service). There are two main processes for the Smishing scams; one involves receiving a text message which is purported to have originated from a known and trusted source, such as your bankers or your system administrator. The second one involves you receiving a vital text message about your identity been stolen or account number been frozen, it then goes ahead to direct you to a website or a phone number for the verification of the account information. The thieves upon receiving the information go ahead to withdraw money from the account or open a new credit card in the victim‟s name. In a similar instance, a vital text message is received by the victim from probably a known or trusted source, which may come along with an attachment. The attachment downloads a virus or malware unto the victim‟s device which in turn installs a root kit or backdoor for the scammers to have access to everything (contacts, inbox messages and application on the phone etc. etc.) on the victim‟s phone and sometimes even have control over it.

2.4.4 Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Search security, 2009).

Unlike a nuisance virus or computer attack that result in a denial of service, a cyber-terrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Apart from that, there is another dimension to cyber terrorism – the use of cyber infrastructure to launder money for financing physical terrorism. In 2005, FBI officials reported that Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases (Tudor, 2011).

Cyber terrorism is said to have taken place when the effects of a widespread computer network attack is unpredictable and might cause enough economic disruption, fear, and civilian deaths, to qualify as terrorism. At least two views exist for defining the term cyber terrorism (Denning, 2009). These are:

1) Cyber terrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.
2) Cyber terrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.

The terrorist‟s use of the Internet and other telecommunications devices is growing both in terms of reliance for supporting organizational activities and for gaining expertise to achieve operational goals. Tighter physical and border security may also encourage terrorists and extremists to try to use other types of weapons to attack the United States. Persistent Internet and computer security

vulnerabilities, which have been widely publicized, may gradually encourage terrorists to continue to enhance their computer skills, or develop alliances with criminal organizations.

They will also probably consider attempting a cyber-attack against the U.S. critical infrastructure (Longe & Chiemeke, 2011). Cybercrime has increased dramatically in past years, and several recent terrorists events appear to have been funded partially through online credit card fraud. Reports indicate that terrorists and extremists in the Middle East and South Asia may be increasingly collaborating with cybercriminals for the international movement of money and for the smuggling of arms and illegal drugs (Denning, 2009). These links with hackers and cybercriminals may be examples of the terrorists‟ desire to continue to refine their computer skills, and the relationships forged through collaborative drug trafficking efforts may also provide terrorists with access to highly skilled computer programmers.

2.4.5 Electronic Spam Mails

These are unsolicited bulk e-mail to multiple recipients. They can be commercial, political, or religious. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, web search engines, and blogs. Spamming is popular because the advertisers have no operating costs beyond the management of their mailing lists and it is difficult to hold senders accountable for their mass mailings. As a result, costs such as lost productivity and fraud are borne by the public and by Internet service providers that have been forced to add extra capacity to cope with the deluge (Longe, & Chiemeke, 2011)

A good example is 419 mails or the Nigerian advance fee frauds which in 1996 was estimated to have cost unsuspecting clientele over five billion dollars These mails emanate in a triangle called the "The Nigerian Connection" mostly in Europe and in some parts of Africa, “The 419 Coalition, 2005.” The Nigerian Scam, according to published reports, is the third to fifth largest industry in Nigeria (Smith, *et al,* 2009).

It is the 419 Coalition views that, in effect, the elites from which successive governments of Nigeria have been drawn are the scammers. Therefore, victims have little recourse in this matter. Monies stolen by 419 operations are almost never recovered from Nigeria. Most 419 letters and e-mails originate from or are traceable back to Nigeria. However, some originate from other nations, mostly also West African nations such as Nigeria, Cameroon, Togo, Liberia, Sierra Leone, Ivory Coast (Cote D‟Ivoire), etc. The effects of such scams have immense effects with confirmed losses of millions of dollars annually (Agboola, 2006).

According to Longe and Longe (2010), governments have tried to come up with policies to try to curtail this menace. Nigeria, through the EFCC, banned night browsing. This is because most fraudulent activities are perpetrated at cyber cafés at nights. For now, there are no quantitative data to measure the effect of this action on the reduction or otherwise of cybercrime in Nigeria. Apart from the availability and usage of Internet facilities in cyber cafes for pornography and other cybercrimes, the evolution of fixed wireless facilities in Nigeria, for instance, has added another dimension to the cybercrime problem. Nigeria therefore enjoys a dubious distinction of being the

source of what is now generally referred to as „419" mails, named after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud.

These crimes are similar to theft and the likes that have existed for century"s offline even before the development of high-tech equipment. Progress in the fight against Internet pornography has been moving at a very slow pace in Africa. A majority of public internet access point deals with the problem in unorthodox manners such as placing notices on cyber cafe walls warning against browsing pornographic sites and other spamming activities. Those with some technical expertise resort to the use of content filters which are downloaded and installed to filter unwanted Internet content (Longe & Longe, 2010).

2.4.6 Cyber Stalking

Stalking in the physical sense generally involves harassing or threatening behavior in which an individual engages repeatedly, such as following a person, appearing at a person's home or place of business, making harassing telephone calls, leaving written messages or objects, or vandalizing a person's property. According to Ellison and Akdeniz (2012) cyber stalking refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person. This term is used interchangeably with online harassment and online abuse. A cyber stalker does not present a direct physical threat to a victim, but follows the victim's online activity to gather information and make threats or other forms of verbal intimidation.

The anonymity of online interaction, they argued, reduces the chance of identification and makes cyber stalking more common than physical stalking. Although cyber stalking might seem relatively

harmless, it can cause victims psychological and emotional harm, and occasionally leads to actual stalking. Cyber stalking is becoming a common tactic in racism and other expressions of hate. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing website (e.g., blogs) and e-mail. The availability of free email and website space, as well as the anonymity provided by these chat rooms and forums, has contributed to the increase of cyber stalking as a form of harassment (Ellison & Akdeniz, 2012).

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat. While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously. The nature and extent of the cyber stalking problem is difficult to quantify. Indeed, current trends and evidence suggest that cyber stalking is a serious problem that will grow in scope and complexity as more people take advantage of the internet and other telecommunications technologies (CCIPS, 2009).

Important advances can only be made if industry, law enforcement, victims, service providers, support groups, and others work together to develop a more comprehensive and effective response to this problem. Ultimately, however, the first line of defense will involve industry efforts that educate and empower individuals to protect themselves against cyber stalking and other online threats, along with prompt reporting to law enforcement agencies trained and equipped to respond to cyber stalking. Physical stalking, online harassment, and threats may be a prelude to more serious

behavior, including physical violence. For example, the first U.S. cyber stalking law went into effect in 1999 in California. Other states include prohibition against cyber stalking in their harassment or stalking legislation. In Florida, HB 479 was introduced in 2003 to ban cyber stalking. This was signed into law in October 2003. The crime of cyber stalking is defined in Florida Statutes 784.048(1) (d) which is one of the strictest such laws in the United States (Smith, 2011).

2.4.7 Fake Copy-Cat Web Sites

One recent trend in on-line fraud is the emergence of fake „copy-cat" web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster"s personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud (www.bbc.co.uk).

2.5 Effects of Cybercrime on Banking

According to Reuter"s media briefs from Cameroon (Cameroon, 2011), British prime minister, cyber-crime costs the British economy some 27 billion pounds a year. On the other hand, the Economic and Financial Crimes Commission Report (2010) ranks Nigeria as third among the top ten sources of cyber-crime in the world. It is estimated that after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent, Nigeria is the next hub of cyber criminals in the world with 8 per cent. The growth of online banking further presents 24

enhanced opportunities for perpetrators of cyber-crime. Funds can be embezzled using wire transfer or account takeover. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems (Atherton, 2010). Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions.

Therefore unless crime detection and prevention are confronted collectively, Nigeria like any other country will remain warm breeding grounds for cartels of such criminal activity. A global effort to combat this crime is of essence. Financial fraud is one of America‟s largest growth industries, creating annual losses of $189 billion (Longe, *et al,* 2010). The cost of application fraud alone, they argued, is more than $35 billion a year. This is by far more damaging than delinquent or bankrupt accounts, fraud losses which are generally three times higher than normal chargeoff rates. This situation poses a real and constant threat to profitability and may raise the price of goods and services for consumers. They further argued that by far, the greatest threats is from ecommerce fraud, identity theft and international criminal organizations, all of which are becoming more widespread and sophisticated every day.

As e-commerce continues to grow, it will become an even bigger attraction for criminals. The report indicated that identity theft is escalating at 40% a year and is particularly problematic compared with more traditional forms of financial fraud. Greater access to credit, an abundance of information, faster electronic communications, and intense competition among financial institutions make it 25

easier than ever for perpetrators to steal identities and falsify information. The existence of cyber-crime and its effects require the formulation of appropriate policies to address them. The next section presents existing policies on cyber- related crime in Nigeria.

2.6 Cybercrime Policy in Nigeria

There is presently no law that is specific to cyber-crime in Nigeria. However, this is not to say that cyber criminals are free to operate in the country. There are general laws that are not specifically related to cyber-crime but are being enforced to deal with the crime. Some of these laws are: the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004, and the Advance Fee Fraud and other Related Offences Act 2006 (Ewelukwa, 2011).

The Nigeria Criminal Code Act 1990 The Criminal Code Act of 1990 (Laws of the Federation of Nigeria, 1990) criminalizes any type of stealing of funds in whatever form, an offence punishable under the Act. Although cyber-crime is not mentioned in the Act, it is a type of stealing punishable under the criminal code. The most renowned provision of the Act is Chapter 38, which deals with "obtaining Property by false pretenses-Cheating." The specific provisions relating to cyber-crime is section 419, while section 418 gave a definition of what constitutes an offence under the Act.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The term methodology is used to describe all activities involved in the collection of the necessary information required for this research work. This chapter describes how the study was designed by indicating the techniques and procedures used for the research and accumulation of data for the study. It comprises the description of the research design, population, sample and sampling techniques, sources of data, instrument for data collection and data analysis and techniques.

3.2 Research Design

This is causal study. A casual study involves an investigation of what causes the other among different variables. Causality approach to this study is most preferred because the study would be investigating whether investment in internet by banks causes increase or decrease in banking profits. This study adopted both descriptive and explanatory research design. First, the study described the trend of bank performance, adoption, use and investment of ICT in banking sector. Second, the explanatory approach was used investigate existing relationship between bank performance and internet, and carefully tests causal research objective of the study.

3.3 Population of the Study

The population was made up of selected staff Fidelity Bank Plc banks. These staff would be selected randomly.

3.4 Sampling and Sampling Technique

Using the purposive sampling technique, the researcher purposively selected a sample size of 100 respondents**.** Therefore, the sample size for the study was 100 respondents.

3.5 Research Instrument

The research instrument used in the study was the questionnaire. A questionnaire is a list of questions to be answered by a respondent to get their views about a subject. It is preceded by a covering letter, introducing the researcher, explaining the purpose of the research and soliciting assistance in providing the required information. (Onweluzo, 2009)

A total number of twenty (20) items were drawn and administered to the respondents. They would divide into two sections; section A will contain items on the demography of respondents and section B consists of items that would answer the research questions as follow:

- Items 1-5 answered research question one.
- Items 6-10 answered research question two.
- Item 11-15 answered research question three.
- Items 16-20 answered research question four.

3.6 Validity and Reliability of the Instrument

The questionnaire that would be used for this study shall thoroughly scrutinize by the supervisor for clarity, precision, and comprehension.

3.7 Data Collection Method

Data were collected through questionnaire which the researcher would be administered face to face to the respondents, 100 copies of questionnaire were distributed to the respondents.

3.8 Method of Data Analysis

Simple tables, frequency and percentage would be adopted in the presentation and analysis of the data generated for the study. These statistical tools were used because they were suitable means of breaking down and analyzing the generated data.

CHAPTER FOUR

DATA ANALYSES AND RESULTS PRESENTATION

This chapter presents the results of the field study; it shows the descriptive information of the respondents, the results of each of the research questions.

4.1 Demographic Analysis of the Respondents

Table I: Demographic Information of the Respondents

Factor	Group	Frequency	Percentage
SEX	Male	43	43
	Female	57	57
	Total	100	100
AGE	18-30yrs	65	65
	31-40yrs	30	30
	41-50 yrs	2	2
	51-60 yrs	2	2
	61 YRS+	1	1
	Total	100	100
YEAR	1-5yrs	48	48
	6-10yrs	30	30
	11-20yrs	21	21
	21yrs+	1	1
	Total	100	100
STATUS	Salary Earners	47	47
	Businessman/woman	26	26
	Student	27	27
	Total	100	100
BANK	Stanbic	4	4
	Gtbank	25	25
	Access	26	26
	First bank	6	6
	Zenith	5	5
	Others	34	34
	Total	100	100

Based on the result on table 4.1 above, it can be observed that about 43 percent of the respondents for this study are male, while, a majority of 57 percent is female. Showing that randomly female are selected more than male probably because the majority of the respondents are female. The age distribution of the respondents showed that about 65 percent of the respondents are between the ages of 18-30, 30 percent of the respondents are in between the ages of 31 and 40, 2 percent fall into the category of 41-50 years and 51-60 years, while 1 percent of the respondents are 61 year above. The implication of this is that, more respondents fall into the age bracket of 18-30 years.

4.2 Analyses of the Respondents Based on Research Questions

Table II: Analysis of Various Cybercrime

		Research Question One				
		SD	D	A	SA	Total
various cybercrime	item1	1	2	24	73	100
	item2	2	2	39	57	100
	item3	1	3	41	55	100
	item4	5	5	36	54	100
	item5	5	4	27	64	100
Total		13	16	167	303	500

From Table II, 97 respondents (97.0%) agrees that e-banking is exposed to cybercrime while 3 respondents (3.0%) disagrees that e-banking is exposed to cybercrime and 96 respondents (96.0%) agrees Phishing greatly affect electronic fraud in the banking industry while 4 respondents (4.0%) disagrees that Phishing greatly affect electronic fraud in the banking industry, 96 respondents (96.0%) agrees that Vishing is considered as a crime in e-banking while 4 respondents (4.0%) disagrees that Vishing is considered as a crime in e-banking, 90 respondents (90.0%) agrees that 31

identity theft is a cybercrime in e-banking while 10 respondents (10.0%) disagrees that identity theft is a cybercrime in e-banking and 91 respondents (91.0%) agrees that disclosure of password or PIN increases cybercrime while 9 respondents (9.0%) disagrees that Disclosure of password or PIN increases cybercrime. This implies that they are the various cybercrime associated with e-banking in Ogun State.

Table III: Analysis Of Cause/Motives Militating Against Effective E-Banking Services

		Research Question 2				
		SD	D	A	SA	Total
causes/motives	item6	8	8	35	49	100
	item7	23	11	38	28	100
	item8	2	13	46	39	100
	item9	6	6	46	42	100
	item10	3	0	36	61	100
Total		42	38	201	219	500

Table III above shows that 84 respondents (84.0%) agrees that users are not well informed or have good knowledge of fraud in e-banking which hinders the effectiveness of E banking while 16 respondents (16.0%) disagrees that Users are not well informed or have good knowledge of fraud in e-banking which hinders the effectiveness of e-banking, 66 respondents (66.0%) agrees that low level of Internet usage by the customers causes e-banking fraud while 34 respondents (34.0%) disagrees that Low level of Internet usage by the customers causes e-banking fraud, 85 respondents (85.0%) agrees that the network providers are not rendering efficient and effective quality of service

for timely report of e-banking crimes while 15 respondents (15.0%) disagrees that the network providers are not rendering efficient and effective quality of service for timely report of e-banking crimes, 88 respondents (88.0%) agrees that lack of strong cybercrime laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught while 12 respondents (12.0%) disagrees that lack of strong cybercrime laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught and 97 respondents (97.0%) agrees that quest for wealth is another cause of cybercrime in Nigeria while 3 respondents (3.0%) disagrees that quest for wealth is another cause of cybercrime in Nigeria. This implies that they are cause/motives militating against effective e-banking services in Ogun State.

Table IV: Perceived Effects Of E-Banking Cybercrimes

		Research Question 3				
		SD	D	A	SA	Total
perceived effects	item11	1	2	52	45	100
	item12	2	5	48	45	100
	item13	1	5	52	42	100
	item14	3	6	41	50	100
	item15	5	5	42	48	100
Total		12	23	235	230	500

From Table IV above, 97 respondents (97.0%) agrees that cybercrime has made banks to create more awareness for customers in backing sector which cost a lot of money on the part of banks while 3 respondents (3.0%) disagrees that cybercrime has made banks to create more awareness for customers in backing sector which cost a lot of money on the part of banks, 93 respondents (93.0%)

agrees fight against cybercrime has increased effective communication between customers while 7 respondents (7.0%) disagrees that fight against cybercrime has increased effective communication between customers, 94 respondents (94.0%) agrees that Cybercrime has made banking verification code effective for customers thereby saving a lot of money that would have gone to the fraudsters while 6 respondents (6.0%) disagrees that cybercrime has made banking verification code effective for customers thereby saving a lot of money that would have gone to the fraudsters, 91 respondents (91.0%) agrees that fight against cybercrime has helped to increase security in banking sector while 9 respondents (9.0%) disagrees that fight against cybercrime has helped to increase security in banking sector and 90 respondents (90.0%) agrees that cybercrime has reduced trust in e-banking transaction by the customers while 10 respondents (10.0%) disagrees that cybercrime has reduced trust in e-banking transaction by the customers. This implies that they are various perceived effects of e-banking cybercrimes.

Table V: Solutions To The Problems Of Cybercrimes That Are Related To E-Banking

		Research Question 4				
		SD	D	A	SA	Total
solutions	item16	1	6	47	46	100
	item17	5	6	50	39	100
	item18	1	2	39	58	100
	item19	3	14	36	47	100
	item20	2	2	18	78	100
Total		12	30	190	268	500

From Table V above, 93 respondents (93.0%) agrees that intrusion detection system can solve the problems of cybercrimes that are related to e-banking while 7 respondents (7.0%) disagrees that 34

intrusion detection system can solve the problems of cybercrimes that are related to e-banking, 89 respondents (89.0%) agrees there are enough cyber security policies to address, detect and punish e-banking offenders while 11 respondents (11.0%) disagrees that there are enough cyber security policies to address, detect and punish e-banking offenders, 97 respondents (97.0%) agrees that there must a risk department with associated technology in each bank to quickly address the report of e-banking fraud cases while 3 respondents (3.0%) disagrees that there must a risk department with associated technology in each bank to quickly address the report of e-banking fraud cases, 83 respondents (83.0%) agrees that my bank updates e-banking software or platform frequently to reduce the cases of e-banking crimes while 17 respondents (17.0%) disagrees that my bank updates e-banking software or platform frequently to reduce the cases of e-banking crimes and 96 respondents (96.0%) agrees that effective cyber security policies should be put in place by government and banks to reduce the attack of crimes committed by the fraudsters in e-banking while 4 respondents (9.0%) disagrees that effective cyber security policies should be put in place by government and banks to reduce the attack of crimes committed by the fraudsters in e-banking. This implies that they are various solutions to the problems of cybercrimes that are related to e-banking.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary of Findings

The study was carried out to evaluates cybercrimes associated with e-banking, the study has the following objectives, to identify various cybercrimes associated with e-banking in Ogun State, to identify cause/motives of e-banking cybercrimes in Ogun State, to determine perceived effects of e-banking cybercrimes and to determine the solutions to the problems of cybercrimes that are related to e-banking.

A total of 100 questionnaires were administered among bank customers in Ijebu- zone of Ogun State. A simple percentage was used as statistic method for the analysis of data and the results serve as the bases of decision making in evaluates cybercrimes associated with e-banking and thus provide more insight on relationship between e-banking and cybercrime thereby adding to the existing body of knowledge.

Consequently, findings from the study showed that:

i. cybercrime exists in the banking sector.
ii. there is a significant relationship between e-banking and cybercrime
iii. e-banking aids cybercrime.
iv. there are factors militating against effective e-banking in Ogun State.

5.2 Conclusion

The Nigerian banking sector has used modern technologies to improve operational competence to enable them remain competitive in the global financial industry. In banking services Industry the Internet Banking is a new era which explores the new horizons of success and development to enhance businesses operations. But unluckily, the evidences from the field work show that, this

innovation comes with certain degree of exposure to cybercrimes and information security breaches which create negative perception towards the bank. The cybercrime definition in relation to the banking services industry can be said as an attack on financial institution resulting in the financial fraud and loss of vital financial data. The literature reveals that, the major issues concerning the financial institution operating within the cyber space have been information security breaches, safety and the lack of trust, fraudulent transactions, robbery and identity theft. In conclusion Nigeria needs strong laws and countermeasures, with combine effort from industrial players, government and the banks as well as cyber security experts to address these societal problems.

5.3 Recommendations

Based on the finding of the study, the following recommendations are made:

1. In order to create and rebuild the trust in banks, there should be proactive cyber and information frame work which should include all employees.
2. There should be public education targeting and educating customers about cybercriminal modus operandi,
3. Financial institutions should publish information concerning data breaches and take steps to correct them.
4. Internet service providers operating in the country should also be mandated to report suspicious traffic going through their networks.
5. The law enforcement agents in Nigeria need to collaborate with their international counterpart to help deal with the cross boarder crime.

REFERENCES

Advance Fee Fraud and Other Fraud Related Offences Act 2006, Laws of the Federation of Nigeria.

Agboola, A. A. (2006). Electronic Payment Systems and Tele-banking Services in Nigeria, Journal of Internet Banking and Commerce, Vol. 11, No. 3, online source.

Atherton. M. (2010). Criminals switch attention from cheques and plastic to internet transactions. The Sunday Times of March 10, 2010.

Anguelov, C. E. et al. (2004). U.S. Consumers and Electronic Banking,1995– 2003. Federal Reserve Bulletin 5.

Balachandran and Balachandher K. G. (2011). "E-Banking Development in Malaysia: Prospects and Problems", 10 JIBL, 250.

Bell. R. Garland. E. & Platt. R.B. (2009). Bridging and signaling subsystems and methods for private and hybrid 15.

Beatson. J.G. (2011). Security - a personnel issue. The importance of personnel attitudes and securityeducation. Proceedings of the Sixth IFIP International Conference on Computer Security.

Cameroon. D. (2011). Cybercrime costs UK 27 Billion pounds, Reuters media briefs.

Chiemeke, S. C., Evwiekpaefe, A. and Chete. F. (2012). The Adoption of Internet Banking in Nigeria: An Empirical Investigation, Journal of Internet Banking and Commerce, Vol. 11, No.3,

CCIPS, (2009) Cyber stalking: A New Challenge for Law Enforcement and Industry. Workshop on the economics of information security.

Crocker. D. (2011). Standard for the format of ARPA Internet text messages.

Denning. D.E (2009). Information Warfare and Security. ACM Press, USA.

EFCC/ NBS/ (2010). Business Survey on Crime & Corruption and Awareness of EFCC in Nigeria, Summary Report.

Ellison. L., & Akdeniz, Y. (2012). “Cyberstalking: the Regulation of Harassment on the Internet,” [2000] Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, pp 29-48. economics of information security

E-Marketer (2013). Estimate and projections. http://www.emarketer.com/docs/emar_whitepaper.pdf Ewelukwa, N. (2011). This Day Newspaper, Nigeria, March 31.2011, PG. 46.

Felson. M. & Clarke. R. V. (2009). Opportunity Makes the Thief. Police Research Series, Paper 98. Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.. London: Home Office. [www.homeoffice.gov.uk/rds/prgpdfs/fprs 98.pdf]

Gaunt. N. (2011). Installing an appropriate IS security policy in hospitals. International Journal of Medical Informatics, 131-134.

IC3/FBI, "IC3/FBI Annual Cyber-security Survey," (2010). [Online]. Available: www.fbi.gov/stories/. [Accessed December 2018].

Jaishankar. K. (2010). Space Transition Theory of Cybercrime. Chapter 14 page 283- 296, Crimes of the Internet by Schallmeger & Pittaro.

Kochems. A. & Keith. L. (2013) Successfully Securing Identity Documents: A Primer on Preventive Technologies and ID Theft.

Kabay. M.E. (2012). Using Social Psychology to Implement Security Policies. In: Bosworth S & Kabay ME (eds) Computer Security Handbook, 4th edition. John Wiley & Sons, Inc., USA,32.1-32.16.

Katsikas. S.K. (2010). Health care management and information system security: awareness, training or education?. International Journal of Medical Informatics 60(2): 129-135.

Kovacich. G.L & Halibozek. E.P (2013). The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program. Butterworth-Heinemann,USA.

Liao Z. & Wong W. K., (2008). The Determinants of Customer Interactions with Internet-Enabled e-Banking Services. The Journal of the Operational Research Society, Vol. 59, No. 9 (Sep., 2008), pp. 1201-1210.

Litan. A. (2014). Phising attack victims likely targets for identity theft. Available: http://www.gartner.com/DisplayDocumen t?doc_cd=120804.

Loftness. S. (2004). Responding to "Phishing" Attacks. Glenbrook Partners.

Longe, O.B. & Chiemeke. S.C. (2011). Cybercrime and Criminality in Nigeria- What roles are internet Access Points in Playing. European Journal of Social Sciences, Volume 6 No 4.

Longe. O.B & Longe. F.A. (2010). The Nigerian Web Content: Combating the Pornographic Malaise Using Web Filters. Journal of Information Technology Impact. Vol. 5, No. 2 Loyola University, United States of America. www.jiti.net.

Longe. O.B. Mbarika. V. Kourouma. M. Wada. F & Isabalija. R. (2010). Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities. International Journal of Computer Science and Information Security. Vol. 6 (3) (pp. 124-135

Martins. A. Eloff. J.H.P (2012). Information Security Culture. SEC 2002: 203-214.

Nitsure. R. R. (2010). E-Banking: Challenges and Opportunities. Economic and Political Weekly, Vol. 38, No. 51/52 pp. 5377-538.

Olasanmi. O. O (2013). Computer Crimes and Counter Measures in the Nigerian Banking Sector. Journal of Internet Banking & Commerce, 15(1), 1-10 http://www.arraydev.com/commerce/jibc/

Ollmann G., "Understanding X-morphic Exploitation," 2010.

Proctor. P.E. & Byrnes. F.C. (2012). The Secured Enterprise: Protecting Your Information Assets. Prentice Hall, Upper Saddle River, USA.

Rachna. D. Tygar. J. & Hearst. M. (2013). "Why Phishing Works" in the Proceedings of the Conference on Human Factors in Computing Systems (CHI2013).

Roger. E.S. (2010). Rogers Communications Inc, 2010 Annual Report APWG (Anti-Phishing Working Group) (2008). Phishing Activity Trends Report. Available: http://www.antiphishing.org.

RSA, "Phishing, Vishing and Smishing: Old Threats Present New Risks," RSA Monthly Online Fraud Report, September, October & November 2009.

Sasse. A. Brostoff. S. & Weirich. D. (2011). Transforming the 'weakest link' a human computer interaction approach to usable and effective security. BT technology Journal 19(3): 122- 131.

Search security (2009). Information Security magazine

Schlienger. T. & Teufel. S. (2012). IS security Culture: The Socio-Cultural Dimension in IS security Management. Proceedings of IFIP TC 11.

Shandilya. A. (2011). Online Banking: Security Issues for Online payment Services. www.buzzle.com/articles.

Siponen. M. T. (2010). On the Role of Human Morality in Information System Security: The Problems of Descriptivism and Non-descriptive Foundations. Proceedings of IS security for Global Information Infrastructures, IFIP TC11 Fifteenth Annual Working Conference on IS security: 401- 410.

Smith. M. (2011). Cyberstalking and the Law.

Smith. S. R. G., Holmes. M.N. & Kaufmann, P. (2009). Nigerian advance fee fraud. Trends and Issues in Crime and Criminal Justice, No. 121. Australian Institute of Criminology, Canberra.Available online http://www.aic.gov.au.

Tudor. J. K. (2011). IS security Architecture, An Integrated Approach to Security in the Organization. Auerbach Publications, USA.

Vroom. C. and R. V. Solms. (2012). A Practical Approach to Information Security Awareness in the Organization. Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, Kluwer, B.V.: 19- 38.

Wood. C.C. (2011). The Human Firewall Manifesto. Computer Security Journal 18(1): 15- 18.

APPENDIX

RESEARCH QUESTIONNAIRE TAI SOLARIN COLLEGE OF EDUCATION, OMU-IJEBU DEPARTMENT OF COMPUTER SCIENCE

Dear Sir/Ma,

This questionnaire is an instrument purposely to gather information on cybercrime associated with e-banking in Nigeria, using Fidelity Bank Plc as the case study. Kindly respond to the questions appropriately. All information supplied will be treated confidentially. Kindly tick (√) only ONE option considered appropriate.

SECTION A

1. SEX: Male ( ) Female ( )

2. AGE OF RESPONDENT: 18 – 30yrs ( ) 31 – 40yrs ( ) 41–50 ( )
51 –60( ) 61years and above ( )

3. YEARS OF BANKING EXPERIENCE: 1 – 5yrs ( ) 6 – 10yrs ( )
11 – 20yrs ( ) 21yrs and above ( )

4. STATUS: Salary Earners ( ) Businessman/woman () Student ( )

5. Name of Transaction Bank: …….....

SECTION B

Kindly tick (√) as considered appropriate.

NOTE: SA – Strongly Agree, A – Agree, D – Disagree, SD – Strongly Disagree

S/N	Statements	SA	A	SD	D
1.	e-banking is exposed to cybercrime				
2.	Phishing (using fake emails and/or fake websites) greatly affect electronic fraud in the banking industry.				
3.	Vishing (using the telephone in an attempt to scam the user to reveal private information, such as bank details and credit card numbers) is considered as a crime in e-banking				

S/N	Statements	SA	A	SD	D
4.	Identity theft is a cybercrime in e-banking.				
5.	Disclosure of password or PIN increases cybercrime.				
6.	Users are not well informed or have good knowledge of fraud in e-banking which hinders the effectiveness of E banking.				
7.	Low level of Internet usage by the customers causes e-banking fraud.				
8.	The network providers are not rendering efficient and effective quality of service for timely report of e-banking crimes.				
9.	Lack of strong cybercrime laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught.				
10.	Quest for wealth is another cause of cybercrime in Nigeria				
11.	Cybercrime has made banks to create more awareness for customers in backing sector which cost a lot of money on the part of banks.				
12.	Fight against cybercrime has increased effective communication between customers				
13.	Cybercrime has made banking verification code effective for customers thereby saving a lot of money that would have gone to the fraudsters.				
14.	Fight against cybercrime has helped to increase security in banking sector.				
15.	Cybercrime has reduced trust in e-banking transaction by the customers.				
16.	Intrusion detection system can solve the problems of cybercrimes that are related to e-banking.				
17	There are enough cyber security policies to address, detect and punish e-banking offenders.				
18.	There must a risk department with associated technology in each bank to quickly address the report of e-banking fraud cases.				
19.	My bank updates e-banking software or platform frequently to reduce the cases of e-banking crimes.				
20.	Effective cyber security policies should be put in place by government and banks to reduce the attack of crimes committed by the fraudsters in e-banking				

Other suggestion(s) to reduce e-banking crime: ……

……...