Fall 2016

Nigerian Internet Fraud: Policy/Law Changes That Can Improve Effectiveness

Anthony Adeoye Adedipe

Nigerian Internet Fraud: Policy/Law Changes That Can Improve Effectiveness

A Thesis Presented in Partial Fulfillment

of the Requirements for the Degree

Masters of Criminology

Anthony Adeoye Adedipe

REGIS UNIVERSITY

August, 2016

NIGERIAN INTERNET FRAUD: POLICY/LAW CHANGES THAT CAN IMPROVE EFFECTIVENESS

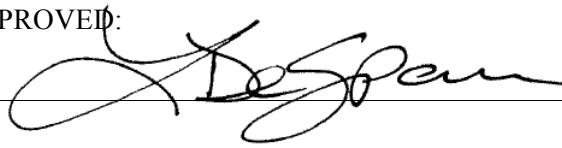
by

Anthony A. Adedipe

has been approved

August, 2016

APPROVED:



Dr. Lynn DeSpain, Faculty/Thesis Advisor

Faculty Chair

Table of Contents

ABSTRACT

Nigerian Internet Fraud: Policy/Law Changes That Can Improve Effectiveness.

This paper presents research about Nigerian Internet fraud and the policy/law changes that can help to prevent it. The paper will further examine some of the relevant legal measures available to help combat cyber fraud in Nigeria. It further highlights the Nigeria 419 scam, which became a major concern for the international community. It is noteworthy that the introduction, growth, and use of the Internet has come with numerous benefits but has also been accompanied by an increase in Internet fraud and other illegal activities. Cyberspace provides numerous opportunities where hijacked emails, anonymous servers and fake websites are being used by scammers to carry out fraudulent activities. The international revolution in ICTs (Information and Communications Technology) has been affected by Nigerian advanced fee fraud on the Internet. Such forms of criminal activities also cover lottery romance and charity scams. Estimates of the losses accrued as a result of cyber fraud are enormous and vary widely. All the Internet frauds are considered as cross-border crime and this paper considers Nigeria as a research study. The paper will conclude by highlighting or discussing some of the measures to monitor or fight the Internet use in illegal activities.

KEYWORDS: PC, Cyber Café, Digital Security, Guilessness, Fraudsters, Virtual Criminal exercise, Detica Report, Cyber Crime, m-commerce (any trading or transaction is held via wireless devices such as cellular phones) and e-crime (criminal activity that involves use of computer or network). NFIC, USCYBERCOM, DOD.

Chapter 1

INTRODUCTION

According to Strassmann (2009), "The Internet or cyberspace alludes to the endless space known as the web. Digital security is the assemblage of guidelines set up perhaps for the protection of internet users." (p. 6). Cybercrime or digital wrongdoing alludes to perhaps to act that attacks both the internet and digital security. The Internet is one of the fastest developing areas of specialized foundation improvement (Strassmann, 2009). Over the previous decades, development of the Internet and its usage has granted everyone an open door. The internet is a world that can provide any information that an individual is searching for. Thus with the birth of the Internet comes an exponentially developing burden of Cyber Crime. Digital security has become a national worry as the risks associated with the Internet become more. (Strassmann, 2009) (p.11-12).

This paper endeavors to give an outline of Cybercrime and Cyber-security. It characterizes the idea of cybercrime and discusses the sources of digital crime and possible ways of eliminating it. This dissertation includes the victims and the purposes behind their contribution. Strategies for stepping up digital security and suggestions that would help in checking the increasing rate of digital crimes will also be highlighted. The paper additionally endeavors to name a few difficulties created by cybercrime to present some solutions to address this problem (Strassmann, 2009, p. 22).

Background of the Study

Personal computer (PC) or Internet fraud can comprehensively be characterized as criminal action, including: gaining unlawful or unapproved access, illicit block attempts, along with specialized methods for non-open transmissions of PC information to, from or within a PC

framework; information obstruction that incorporate unapproved harming, cancellation, weakening, adjustment or concealment of PC information; frameworks that meddle with the working of a PC framework by inputting, transmitting, harming, changing or stifling PC information; abuse of gadgets, imitation (identity theft), and electronic extortion.

The Internet has given a place of refuge for fraud as a window of opportunities to commit internet scam. One of these countries is Nigeria with other individuals from various places in the world who can now relate to each other by openly connecting to and using the points of interest offered by Internet. Data innovation unrest connected with the web in Nigeria has created numerous cases of crimes or criminal activities. “The very few criminally minded youth in the nation, who are for the most part not learned or graduates, are taking and perpetrating outrage through the use of web online business trades” (Strassmann, 2009, p. 1-2),. The administration of web online business, which normally is expected to be a gift since it allows people to have considerable opportunities of chances in different fields, is quickly turning into a wellspring of inconvenience and stress because of the abominations being executed through it. Such issues have raised questions about the security of cyberspace in Nigeria.

Problem Statement

In as much as some of the earliest fraud cases trace back to 1996, the claims of Internet fraud were not as detailed as those noted in 1997. There were very minimal details to support such claims. Nonetheless, it was not until 1997 that numerous cases concerning Internet fraud became documented and available in the public domain, according to Internet Fraud Watch. Since 1997, many cases have arisen and numerous types of crimes multiplied, and the methods of committing such criminal activities over the Internet have also evolved to a great extent. In fact, in 2002 alone, the Internet Fraud Compliant Center reported 75,000 complaints, which

indicated that cases multiplied greatly in just one year after 2001. The amount of money lost as a result of the scams also grew exponentially in millions of dollars. This clearly indicates that Internet fraud and its evasiveness from law enforcement is a rapidly growing problem.

First, Internet usage has attracted many consumers and made online buying and selling of products a comfortable platform with numerous e-commerce practices. Secondly, e-commerce has reached a level whereby it is likely to match m-commerce (any trading or transaction held via wireless devices e. g. cell phones), nonetheless; there is no professional or governing authority with the ability to monitor and certify web content. This creates one of the biggest problems for lack of control when it comes to Internet fraud (Strassmann, 2009, p. 4).
From business, industry, and government to non-revenue driven associations, the Internet has improved business procedures, such as, sorting, outlining, coding, altering, and modification. Nevertheless, it has likewise brought unintended results, enabling cybercriminals to engage in activities such as spamming, credit card fraud, ATM fraud, phishing, criminal exercise, and wholesale fraud.

This paper describes the development of a new war or Internet fraud problem which will bring about annihilation of more noteworthy size than the two past World Wars, it has been realized that Nigeria has been a receptive nation since the introduction of the web. The extraordinary episodes of digital wrongdoing in Nigeria are entirely problematic, and the negative effect on the socio economy of the nation is exceedingly exasperating. In the course of recent years, indecent Internet users have kept on utilizing the web to perpetrate wrongdoings; this has evoked blended sentiments of deference and apprehension in the general masses alongside a developing unease about the conditions of digital and individual security. These

indecent Internet users have seen refined remarkable increments with individual government coming up with laws that would secure the Internet and its users.

According to Strassman 2009, the problem is that the Internet is insecure. The most dangerous method for disabling networks is to insert somewhere in the communication links "spyware" (software that surreptitiously tracks or transmits data to a third party) or, "botnets" (software robots that allow an unauthorized user to control compromised servers). The inherent insecurity of Internet and of inevitable human lapses by the network defenders makes that possible. (p. 8). Cybercrime is definitely the biggest problem that Nigeria also faces. Before the year 2001, the marvel of digital wrongdoing was not comprehensively connected with Nigeria. From that point forward, in any case, "the nation has gained an overall reputation in Internet criminal exercises, particularly money-related scams" (Strassmann, 2009, p.10), conducted over the Internet, Nigerian digital lawbreakers are every day formulating better approaches for executing this type of wrongdoing, and the current strategies for following these offenders are no more reasonable for managing their emergent tricks. The casualties also demonstrate expanding naivety and guilelessness at the prospects prompted by these fraudsters. Since the issue of digital security is bringing up various issues in most people's minds in Nigerians, it is not out of the question that this paper assists in offering answers to these inquiries. This thesis tries to give a review of digital wrongdoing and digital security, outline a few difficulties and proffer solutions.

Research Questions

There are numerous questions that this research tries to answer. In this study, the major objectives are to respond to the questions listed below. In fact, it focuses on addressing the issue of the vulnerability of Nigerian society when it comes to crimes and abuses on computer

networks and the international technological infrastructure as a whole. Some of these questions include:

i. What is the extent that Internet fraud and related economic crime affect Gross Domestic Product of Nigeria?

ii. What is the extent by which Internet fraud and related financial crime affect inflation in the economy of Nigeria?

iii. How are cyber-crime and cyber security threats in Nigeria tackled by the relevant authorities?

iv. How effective and efficient are the efforts taken to ensure cyber security in Nigeria.

v. What are the solutions, and what can be done to improve the state of cybercrime and cyber security in Nigeria?

Significance of the Study

This study is significant because addresses some very important issues associated with Internet fraud and its evasiveness from law enforcement. First and foremost, this study aims at combating the growing cases of cyber crimes or Internet fraud in banking institutions in Nigeria. The study will lead to a deeper understanding of the various types of Internet fraud currently in existence. The findings of this research will serve as decision variables or inputs for managers, bankers, and government agents. The policy makers and professionals in the relevant fields will find the research useful for their policy making, and the study will create more awareness in the minds of readers about credit card and money transfer fraud (Augustine, 2010, p. 3).

Given those characteristics, it is imperative for nations to make plans towards fighting against Internet fraud, especially online fraud, which is all over the world. The incidence of online crime has grown considerably in recent years, with terms such as malware, Trojans,

botnets, and phishing attacks entering the common vernacular. “This significant increase in activity might best be described as international commercial sabotage but, some would label it more sensationally as cyber fraud” (Strassmann, 2009, p. 10). One of the increasingly significant tools in the arsenal of attackers is the spear phishing attack. This malware involves sending a fraudulent, yet convincing, e-mail to a targeted individual within an organization who has a position of authority or access to sensitive systems (Augustine, 2010, p. 7). Unlike traditional phishing schemes, however, the message appears to come from within the organization or an individual in a position of authority to increase the likelihood that the recipient will open the e-mail. Also, the message will demand information from the victim and request the individual to download or open a keylogger, spyware program, or some other type of malicious software to gather sensitive information surreptitiously. Spear phishing is less likely to be used by hackers, instead being employed by sophisticated groups out for financial gain, trade secrets, or military information (Augustine, 2010, p. 7).

Statement of Objective

As much as the reality of the matter is, digital offenders can utilize Internet innovations to focus on all forthcoming online clients and business exercises. Certain demographic client classes might be more defenseless than others. Some business applications may likewise be more inclined to extortion. This study analyzes the multiplication of Internet misrepresentation for the period 1998 through 2014. In particular, the variables inspected incorporated the classifications of online extortion, installment techniques utilized for conferring those tricks, the affected victims, and patterns, assuming any (Augustine, 2010, p. 6). Information which relates to procedures, applications, of the victims that are harmed can help administrative organizations to be more viable in their requirement endeavors and to give the best possible exhortation the general population may require. From this research, there will be a significance of online

frameworks of individual that require PC data framework, security configuration and improvement (Strassmann, 2009, p. 5). Teachers, specifically, can utilize the results reported in this study for the improvement and configuration of new educational programs and course content that can minimize PC violations. Furthermore, perhaps simply "the means used by the perpetrators of Internet fraud can be used to teach students can likewise be utilized to teach students about the dangers connected with online exercises (Augustine, 2010, p. 19).

Chapter 2

LITERATURE REVIEW

Strassmann (2009), states that the "issue of Internet fraud is one that has been examined by numerous individuals with different viewpoints, most coming from various people with diverse perspectives.(p. 4)". Digital fraud has gone past traditional crimes and is now causing debilitating repercussions for the national security of all nations, even for some nations that are technologically advanced such as the United States. He also emphasized that "the reception by all nations of proper enactment against the abuse of Information and Communication Technology (ICT), for criminal or different purposes" (p. 7). However, (Adebusuyi, 2008), also stated "that including exercises planned to influence the respectability of national basic data foundations, is vital to accomplishing worldwide digital security." (p. 372)

Strassman (2009), further expressed that "since dangers are likely to affect any place around the world; the difficulties are intrinsically worldwide in degree and thus require universal participation, investigative help, and basic substantive and procedural ways of doing business online." (p. 7). In accordance with the above, Professor Augustine Odinma(2010), states that "Internet fraud or cybercrime is any illicit activities executed in, on or through the web with the plan to cheat, dupe or cause the glitch of a system gadget, which may incorporate a PC, telephones, and so on (p. 20). The illicit activities might be aimed at a PC system or gadgets e.g., PC infection, and denial of service attacks (DOS) or malware (noxious code). The unlawful activities might be encouraged by PC system or gadgets with target autonomous of the PC system or gadget.

Relating digital wrongdoing to the military in a paper portraying his personal stake in the nation's military prosperity, Major General Umo traced cybercrime, digital terrorism, digital fighting and digital security are one and the same thing (Adebusuyi, 2008, p.375). Strassmann, (2009), also indicated that

"the most significant change in military policy is the re-designation of the position of the Director, of the National Security Agency (DIRNSA) who is also the Commander of USCYBERCOM. This brings both organizations with cyber security expertise under a unified military command. The purpose of the combination of USCYBERCOM and NSA is to deliver to DOD (Department of defense) a well-protected information infrastructure (p. 3). Longe (2011) also emphasized that "cyber-deception and theft involves deception and stealing with the use of technology. Typical examples are credit card fraud, intellectual property violation and piracy. Cyber deception and theft comes in various forms, some of which is outline as to the wrongful acquisition and use of someone else's personal data in some way that involves fraud or deception, typically for economic gain" (p. 171)

This account of taking or imitation of an individual or an association is synonymous to taking up arms against the objective of the crime. Giving more insights on how such crimes can be contained, since survey indicated that human action contributed more to security failure than technological weaknesses, more people needs to be educated to understand security threats, vulnerabilities and other breaches (Adebusuyi, 2008, p. 368). The question whether cyber attacks are an act of war is still being debated. Regardless of that Internet security must be fused with conventional warfare. Everyone not only a selected class of cyber war specialists is now engaged in Internet warfare. The transfer of the responsibility for network assurance from the Armed Forces and Agencies to the USCYBERCOM is a necessity. The consolidation of cyber security under a single unified command is required to overcome the organizational disconnects that currently prevail in DOD. This chapter highlights related literature on the problem of Internet fraud and its evasiveness from law enforcement in Nigeria as a case study (Strassmann, 2009, p. 7-10).

Defining Cyber Fraud and Evasion of Law Enforcement

The major problem that arises when it comes to analyzing cybercrime is that it lacks a dependable and legal meaning for the activities that may constitute cybercrime. According to numerous authors, "the definition of cybercrime creates numerous theoretical multifaceted issues (Adebusuyi, 2008, p. 368)." This is due to the fact that there are numerous definitions of cybercrime and other related terminologies (Augustine, 2010, p. 16). What makes it even more complex to understand the meaning or the right definition of cybercrime is that there are numerous related terms such as information technology crimes, digital crime, computer-related crime, and computer crime (Adebusuyi, 2008, p. 370). Some people refer to it as Internet crime, e-crime, net crime and virtual crime. However, despite all the issues that arise with the definition of cybercrime, it is noteworthy that cybercrime may reasonably be defined as numerous criminal activities and offenses perpetrated through the Internet or cyberspace (Augustine, 2010, p. 16).

During the 10th United Nations Congress on Prevention on Crime and Treatment of Offenders, which was a workshop aimed at assisting in address issues associated with computer networks, cybercrime was categorized into two main categories.

The first definition was based on a narrow sense of cybercrime and was defined as illegal behavior perpetrated through electronic means targeting the security of computer systems and the information processed through computers (Adebusuyi, 2008, p. 376). The second definition of cybercrime was based on a broader sense and referred to illegal conduct committed through a computer system or network, including such crimes as illegal possession or distribution of information through computer networks or systems (Augustine, 2010, p. 11). Besides these two definitions, a conceptualization of cybercrime as those "PC interceded exercises which are either unlawful or considered illegal by specific groups and which can be led through worldwide electronic systems." (p.13). The working definition for cybercrime by the Canadian Police

College has progressively been acknowledged by Canadian law implementation offices; "as a criminal offense, including a PC as the object of wrongdoing, or the instrument used to carry out a material part of the offense" (Adebusuyi, 2008, p. 369). The expert proposed a definition for cybercrime that includes all unlawful exercises where PCs, PC frameworks, data systems or information are the objective of wrongdoing and those known illicit exercises or wrongdoing that are effectively carried out through or with the guide of PCs, PC frameworks, data systems or information. It is noteworthy that there is no reliable and statutory definition for cybercrime (Adebusuyi, 2008, p. 369-372).

Law Enforcement and Prosecution

The Internet performs a number of important functions, and for most people, it is beneficial more often than harmful. This was better clarified by Mrs. R. Moses Oke when she said "The oxymoronic way of the Internet is one of its unexpected attributes; at its commencement, nobody, maybe, could have obviously predicted that and how, the Internet would sometimes turn into a veritable stage for globalized criminal exercises" (Adebusuyi, 2008, p. 376). As it has been bountifully commented, the advantages of the Internet have in many cases been spoiled by its flexibility for virtual criminal exercises that have limitless, devastating physical and social effects. Numerous people will concur that worries are expanding as Nigeria is expanding its digitalization not just in the range of business and interchanges, but also step by step into the zone of electronic banking. In the previous year, banking electronically and the cashless activity have been on the center stage (Adebusuyi, 2008, p. 376).

Amaka Eze's (1995) article for THIS DAY live indicates, "As the nation coordinates electronic payment framework into its budgetary foundation; a stage that is relied upon to quicken the country's e-trade development, the negative effect of Internet fraud on organizations,

and the nonappearance of proper laws to ensure the lawfulness of online businesses, keep on creating dread in the psyche of clients and potential online clients" (para. 11). Indeed, even as discussed the ascent and perils of digital crimes and rupture in digital security (Adebusuyi, 2008, p. 377); it is vital to concentrate on approach to minimize or totally kill its occurrence in Nigeria. Nigeria is one of the examples in Africa where cybercrime has proliferated to a "higher degree" or "level." To reestablish the full radiance of digital security, those with the intention of helping minimize this menace need to invest energy to figure out how cybercrime rings works and after that device methodology to battle the dangers presented by cybercrime. It is noteworthy that people are unlikely to battle today's crimes with yesterday's innovation. It will dependably be a losing fight if security experts are behind digital hoodlums regarding technological information. All efforts must be directed towards the processing abilities, as well as IT Security skill, that must be combined to ensure that this menace is addressed fully (Adebusuyi, 2008, p. 373).

Likewise, numerous people continue to talk about expenses caused by the legislature because of the ascent of digital crime;

- The Detica report is a major resource and piece of research that reveals, all measuring digital crime originated from organized crime groups in Nigeria is 80 percent.
- Antivirus programming, protection, consistency; costs as an outcome of Internet fraud,
- Direct misfortunes and backhanded costs, for example, debilitated intensity as an aftereffect of licensed innovation bargain; costs in light of Internet fraud,
- Remuneration installments to casualties and fines paid to administrative bodies; aberrant costs, reputation harm to firms, loss of trust in digital exchanges by people
- Organizations lessened public incomes
- The development of the underground economy.

Having seen cybercrime from alternate points of view, we would now talk completely about digital wrongdoing, digital security, occurrences and arrangement components in the accompanying segments. Much has, as of now been finished by the law requirement operators, however, digital wrongdoing is still executed underground and many people cannot figure out when it is being done (Augustine, 2010, p. 12).

Emerging Cyber Tricks in Nigeria

Nigeria is the best case study for understanding the multifaceted nature of Internet fraud. Studies show that it is a home where Internet fraud are executed and where there are numerous emerging tricks that cyber criminals are using to lure people to fall into their traps. Some well-known tricks include;

i. Online Charity is an aspect of e-crime that is very common in Nigeria. It is a situation whereby fraudulent individual host websites of charity firms to solicit financial donations for organizations that do not really exist. It is very unfortunate that so many unsuspecting well-wishers and people willing to donate have succumbed to such tricks (Adebusuyi, 2008).

ii. Another scam involves winning lottery tickets that a person never entered. This is an approach whereby scams send messages to unsuspecting people that they have won tickets that they never participated in. One of the notable scams that were reported recently involved the State Department's green card lottery.

iii. The beneficiary of Will Scam is another form of scam. This is a situation where cyber criminals send you an email that a person or the victim has been named the beneficiary in the will of an estranged relative, and it indicates that the victim stands to win an estate worth millions of dollars (Adebusuyi, 2008).

iv. The other category is Next of Kin Scam, which entails a number of issues such as collecting money from different banks and transfer fees by luring the clientele to claim an inheritance of millions of dollars from a Nigerian bank that belongs to the relative that has died.

v. Internet/Computer Service Time Theft is a scam whereby children in Nigeria have developed a way of linking Cyber Cafes to the network of some ISPs in a manner that is undetectable by the ISPs and that allows the Cafes to work without paying such charges (Adebusuyi, 2008).

vi. Taking over victims personal or checking accounts. This is usually done by internet criminals upon receipts of victim's identifications and creates a phony address where they can receive victims check books and siphoned all the money from their account.

vii. Lottery scams cause users to believe that they are the beneficiaries of an online lottery, which is usually a scam because such lotteries are non-existence (Adebusuyi, 2008).

Nigerian 419

According to Taylor (2015), The "419" is a section of Nigeria criminal code not just for the internet scam alone but for other types of financial and fraudulent transaction and scam since the early 1980's (Taylor (2015) within the country. The "419" was enacted as a criminal code when the offenders will send out letters to people who have applied for crude oil allocation from NNPC stating that their allocation has been approved. They will then request for funds to complete the transactions with both NNPC and Central Bank of Nigeria. Many people fell victim of the scammers. The Internet scam was added as part of the criminal code after 1986. The Nigerian government is not sympathetic to victims of these schemes since the victim actually conspires to remove funds from Nigeria in a manner that is contrary to Nigerian law. The

schemes themselves violate section 419 of the Nigerian criminal code, hence the label “419 frauds” (p.100)

The indictment of such criminal movement is confounded and can regularly be sidestepped by Internet criminals. Thus, reports of such wrongdoing still show up in the online networking and online groups, e. g. 419 scam.org sites that sites that exist to relieve the danger and help clients to distinguish trick messages (Adebusuyi, 2008). These days, 419 scams are frequently seen as a specific kind of spam. Though, the majority of this spam is presently sent predominantly by botnets (malware) and by traded off machines in mass amounts, Nigerian trick exercises are still generally performed physically. Additionally, the hidden business and operation models vary. Spammers trap their casualties through building exertion, though con artists who depend on human components: compassion, voracity, and social designing methods. Con artists utilize exceptionally primitive devices (assuming any), in contrasted with another type of spam where operations are regularly totally automated (Adebusuyi, 2008). Despite the fact that today 419 scam messages are overshadowed by the huge amount of spam sent by botnets, they are still an issue that causes generous money related misfortunes for various casualties all around the globe (Oghenerukevbe, 2008, p. 7).

An advance charge trick is a kind of extortion and a standout among the most well-known kinds of certainty traps. The trick ordinarily includes promising the casualty a noteworthy offer of a substantial total of cash, consequently for a little in advance installment, which the fraudster requires so as to acquire the extensive whole (Adebusuyi, 2008). In the event that a casualty makes the installment, the fraudster either imagines a progression of further charges for the casualty, or essentially vanishes. There are numerous minor departures from this sort of trick, including the 419 trick, the Spanish Prisoner trick, the dark cash trick and the Detroit-Buffalo

trick (Oghenerukevbe, 2008). The trick has been carried out over fax and by traditional mail and is, and is presently predominant in online correspondences like messages. Online renditions of the trick originate mainly from the United States, the United Kingdom, and Nigeria, Togo, South Africa, and Benin, with the Ivory Coast, the Netherlands, and Spain also having high frequencies of such misrepresentation (Adebusuyi, 2008). The scam messages frequently claim to be from Nigeria, yet for the most part, this is not valid. (Laura, 1995, p. 201)

Internet criminals will recount to the victims an intricate fake anecdote about a lot of cash "caught" in national banks amid common wars or upsets, typically in nations presently in the news (Laura, 1995). On the other hand, they may let the victim know about a huge legacy that is "hard to get from a direct result of government confinements or duties in their nation" (Adebusuyi, 2008). The criminals may reach their victims by email, letter, instant message or long-range informal communication message (Oghenerukevbe, 2008). Criminals offer their victims a vast aggregate of cash to help them exchange their own fortune from their country. These tricks are regularly known as "Nigerian 419" tricks in light of the fact that the principal wave of them originated from Nigeria (Oghenerukevbe, 2008). These tricks now originate from all over the world (Oghenerukevbe, 2008). Criminals may request your ledger points of interest to "help them exchange the cash" and utilize this data to later take your assets (Laura, 1995). On the other hand, Internet fraudsters may request that victims pay expenses, charges, or duties to discharge or exchange cash out of the nations through victim's banks (Laura, 1995). These expenses may even begin as very small sums. On the off chance that they are paid, the trickster may make up new charges that require installment before you can get your prize. They will continue requesting more cash for as long as you will part with it (Adebusuyi, 2008).

Challenges of Cyber Crime

Most nations do not believe that any changes or improvements are foreseeable as necessary to regulate the proliferation of Internet fraud. If a cyber café is closed down today in a geographical area in Nigeria, more will populate in another area the following day. There are more people with fraudulent brain in Nigeria than educational. Most of the 419 operators are none educated and there is no employment. Thus this is all they know as a means of making money.

Many people are affected financially, and the country also loses a lot of financial capability from such scams because they put the innocent citizens into tricky situations after they have been robbed of their hard earned money. Some of the challenges presented by such scams are emphasized below.

One of the challenges presented is that the rate of the crime has grown exponentially such that it goes beyond the healthy Internet usage in Nigeria. (Laura, 1995), for example, an ICT security consultant who is also a member of the Nigeria Cyber Crime Working Group (NCWG), Tunji Ogunleye, indicated that the rate of e-crime in Nigeria has outgrown the rate of usage of the Internet and is also third in the fraud attempt category .This is a major challenge that is affecting most Nigerians and those visiting the country because they have fallen into such hands at some point. This consultant indicated that Nigeria is 56th out of 60 ranked nations with regard to embracing the Internet and stands third in the fraud attempt category (p.207). Many people are wondering why e-crimes have increased exponentially in Nigeria, and probably the relevant agencies should look at the reason behind Nigeria's vulnerability (Adebusuyi, 2008).

Charles Emeruwa (2005), stated that "another challenge in Nigeria is corruption; Nigeria was ranked third among the most corrupt nations globally" (p. 2). Until 1999, defilement was

seen as a lifestyle in Nigeria. The other challenge is the lack of standards and national central control and about this, Charles Emeruwa, an expert to Nigeria Cyber Crime Working Group (NCCWG), emphasized that the absence of directions, norms, PC security, and insurance all act to hamper genuine e-business (Oghenerukevbe, 2008). Outside Direct Investment (FDI) and remote outsourcing are empowering PC abuse (Laura, 1995). Nigeria also lacks the necessary infrastructure that can properly observe and capture calls, Information and Communication Technology gadgets (Laura, 1995).

Another one is the lack of national functional databases: In this regard, the national database could serve as a method for finding the culprits of these grievous demonstrations by registering with past individual records and following their developments (Anderson, et al. 2012). Another challenge is the proliferation of cybercafés: As a method for being the breadwinner to the family, the young entrepreneur has become involved in cybercafés that serve as delighted shelters for the syndicates (Oghenerukevbe, 2008). The porous nature of the Internet poses additional problems: The Internet is free for all with no focal control.

Additionally, Nigeria also lacks both the domestic and foreign law enforcement agencies that can be employed to monitor hostile Internet usage abroad and locally. A threatening group utilizing an Internet associated PC miles away can attack web associated PCs in Nigeria as effortlessly as though they were closer to the computer (Laura, 1995). It is regularly hard to recognize the culprit of such attack, and notwithstanding when a culprit is distinguished, criminal arraignment across over national limits is tricky and to some extent impossible (Anderson, et al. 2012). The issue of unemployment is another challenge of e-crimes. The spate of unemployment in Nigeria is disturbing and developing by the day. Organizations are collapsing and money-related establishments are going bankrupt. The government has proposed a mass sack of

government specialists (Oghenerukevbe, 2008). Organizations are likewise setting out on mass sacks of staff. Money related organizations have put age limit requirement on who is qualified to apply for employment thereby creating massive lay-off of employees (Oghenerukevbe, 2008). The destitution rate is another challenge attributed to cybercrime. On a worldwide scale, Nigeria is viewed as an underdeveloped nation. The poverty rate is perpetually expanding. The rich are getting wealthier and the poor are getting poorer. (Anderson, et al. 2012)

Overview of Cyber Crime and Cyber Security

As much as innovation has grown exponentially, the meaning of the Internet, digital security, and Internet fraud have also changed over time. It has been contended that since internet crime may include all classes of wrongdoing, a definition must underline the distinction, the information or the utilization of PC innovation. The Internet alludes to the endless space known as the web (Anderson, et al. 2012). It alludes to the related system of data, and innovation segments that support a number of our interchanges set up today. Digital security is the gathering of instruments, arrangements, security ideas, security shields, rules, activities, preparation, best practices, hazard administration approaches, certification and advancements that can be utilized to protect the digital environment, association and client's advantages (Oghenerukevbe, 2008). Association and client's benefits incorporate associated processing gadgets, faculty, base, applications, administrations, information transfers, frameworks, and the totality of transmitted and/or put away data in the digital environment. Digital security endeavors to guarantee the fulfillment and upkeep of the security properties of the association and client's advantages against applicable security dangers in the digital environment (Oghenerukevbe, 2008).

Digital security is the assortment of standards set up to ensure the safety of the Internet. In any case, as we turn out to be more subject to the Internet, we without a doubt confront new

dangers. Digital wrongdoing alludes to the arrangement and separation of wrongdoing assaulting both the internet and digital security. In fact, modern digital cyber criminals, present dangers to Nigeria's economy and national security. Anderson, et al. 2012) indicates that Nigeria's financial stability and national security rely upon an unlimited mineral resource such as crude oil, frameworks, administrations, and assets known as the Internet. The Internet has changed the ways we share information, travel, control our homes, run our economies (Anderson, et al. 2012). Digital security is the assemblage of innovation, procedures, and practices intended to ensure systems, PCs, projects and information from assaults, harm, or unapproved access. In processing or digital connection, the word is synonymous with cyber-security (Oghenerukevbe, 2008). Guaranteeing digital security requires facilitated endeavors from both the nationals of the nation and the nation's data framework (Oghenerukevbe, 2008). The risk posed by ruptures in our digital security is progressing more quickly than we can stay aware of it. It is unrealistic to focus endeavors on one and only part of the break as it means carelessness and recompense of development for different parts of the rupture (Anderson, et al. 2012, p. 124). This leads to the reason why all nations need to combat digital security breaks overall.

Digital wrongdoing alludes to criminal action done by utilizing PCs and the Internet. This incorporates anything from downloading unlawful music records to taking a huge number of dollars from online ledgers (Oghenerukevbe, 2008). Cybercrime additionally incorporates non-money related offenses, for example, making and dispersing infections on different PCs or posting secret business data on the Internet (Oghenerukevbe, 2008). Maybe the most conspicuous type of Internet fraud is wholesale fraud, in which culprits utilize the Internet to take individual data from different clients. Maybe the most complete definition of cyber-wrongdoing is, "A criminal action including a data innovation foundation, including unlawful access

(unapproved access), illicit block attempt (by specialized method for non-open transmissions of PC information to, from or inside a PC framework), information obstruction (cancellation, crumbling, adjustment, unapproved harming or concealment of PC information), frameworks impedance (meddling with the working of a PC framework by inputting, transmitting, harming, erasing, breaking down, changing or stifling PC information), abuse of gadgets, deceptive (ID burglary), and electronic extortion" (Anderson, et al. 2012, p. 125).

Complexities of Cybercrime

The issue of Internet fraud is very complex to a greater extent, however; the speed and immense power of the Internet and technological development puts many countries in a quagmire. The rate and the level at which present-day data innovation convolutes the location and examination of PC violations are worrying (Anderson, et al. 2012). For instance, networks for communication now traverse the globe, and a single PC can without much of a stretch interface with destinations that are situated on various sides of the equator (Oghenerukevbe, 2008). This brings extremely critical issues up regarding purview, accessibility of evidence, co-appointment of the examination and the legitimate framework(s) that can be connected to criminal acts that happen in such a setting (Oghenerukevbe, 2008). New innovations make new ideas that have no lawful equality or standing. Nonetheless, a virus uses the assets of the contaminated framework without the proprietor's authorization (Oghenerukevbe, 2008). Subsequently, even a generous infection might be differently translated as a framework infiltration, a bit of electronic graffiti, or essentially a disturbance trick (Oghenerukevbe, 2008). The significant point, in any case, is that the legitimate framework and along these lines, the meaning of PC wrongdoing itself is receptive and not able to subsume practices or acts that include new computational ideas (Oghenerukevbe, 2008). Data has a few exceptional and

theoretical properties, for instance, its ability to remain in the proprietor's possession after it has been replicated or stolen (Oghenerukevbe, 2008). The most recent decade has seen the legitimate framework battle with the ramifications of this in a PC based connection (Anderson, et al. 2012).

Obviously, routine notions of copyright, patent rights and burglary have been strained when connected to programming and PC based data fundamentally, in light of the fact that current ideas of robbery and break-in, for instance, identify with basic ideas of lasting hardship or evacuation (burglary) or physical harm (break-ins). A related property of advanced data is the straightforwardness and degree to which it can be changed and deciphered. It can be spoken of as project content (the source code), executable code (pairs), or it can be changed in an expansive number of ways scientifically, by encryption, or by transformation to say a holographic picture or a bit of music. For whatever the length of time that the method(s) of change are known, the music, the picture, or scrambled content can be made into an interpretation of the back to its unique structure. Consequently, the educational structure in which data exists may inevitably have no lawful status (Anderson, et al. 2012). Rather, some measure of its quality or usefulness as data itself may, in the long run, decide its lawful and business position. This flexibility of data has suggestions regarding framework break-ins where data may not be wrecked (as in defiled or eradicated), but rather is scrambled or made briefly blocked off. Such activities can barely be named as vindictive harm (Anderson, et al. 2012).

Effects of Cyber Crime

There are numerous effects of cyber crime on citizens, victims, and the nation at large. Some of the effects are the financial loss, whereby cyber criminals work like terrorists, and most of their actions are never beneficial to the society. Individuals living in these societies are also affected by the financial losses incurred as a result of cyber criminals or frauds. A country like

Nigeria has also lost its reputation because it is the highest ranked globally when it comes to cybercrime cases (Anderson, et al. 2012). The loss of reputation also discourages numerous countries from doing business in such bad business environments. They usually fear that they are likely to be defrauded or faced with criminal activities, which makes them lose numerous clients. Numerous cases of cyber crimes are likely also to reduce productivity since a lot of efforts are vested in the creation of awareness for unsuspecting clients. Productivity also goes down because cybercrime forces people to focus mostly on prevention measures that can help to address the problem of cyber crime and losing focus on increasing production. Another problem is the vulnerability of their Information and Communication Technology (ICT) systems and networks, which is usually exposed to the offenders (Anderson, et al. 2012).

Solutions to Cyber Crime

The main way Nigeria can take care of its numerous issues associated with Internet fraud is by giving youths more opportunities to take an interest in the administration, the economy, and society at large. Youngsters are the prime recipients of school change and the rate of youth in higher learning institutions is right now high (Anderson, et al. 2012). In the event that youths were in control, the instructive framework in Nigeria would not be in its present state, and unemployment would be lessened greatly (Olumide & Victor, 2010). However, when it comes to Internet fraud, many authors have suggested various ways of addressing the problem. In the meantime, youths should not sit tight for good things to come to them, but instead need to take the singular activity to ensure that they succeed in life and not engage in cyber frauds. Strengthening youths and activity will enhance life for all Nigerians. Nigerian government authorities and different elites need to impart energy to the nation's youth and listen to youthful groups' thoughts for how to better the nation. The young fellows and ladies of Nigeria are

tomorrow's senior citizens and, if included, could change Nigeria (Olumide & Victor, 2010). Without the vitality of youth, society will rot and die. Notwithstanding minimizing of debasement in the nation, Nigerians ought to develop the propensity for being persistent. The reason why people become involved in criminal activity is that they are worried and practices are on the grounds that they are worried and need to profit. In some nations of the world like the United States, numerous Nigerians are held in penitentiaries and some have been murdered on account of the degenerate practices they committed (Anderson, et al. 2012).

Laying emphasis on education is a very vital way of ensuring that the society grows upright and could also help reduce levels of Internet frauds. Training is an important way of addressing cybercrime (Olumide & Victor, 2010). In fact, Internet fraud in Nigeria is hard to demonstrate as it does not have the customary paper review trail, which requires the learning of authorities in PC innovation and web conventions. It is, therefore, important to instruct students that if they are going to utilize the web, they have to consistently keep up and redesign the security of their framework. It is additionally essential to teach companies the best practices for effective security for compelling security administration (Anderson, et al. 2012). For instance, some expensive associations now have an approach that all frameworks in their domain must meet strict security rules (Olumide & Victor, 2010). This is an important way of ensuring the security of their clienteles' information. Computerized redesigns are sent to all PCs and servers on the inner system, and no new framework is permitted online until it fits in with the security strategy employed in the system (Olumide & Victor, 2010). The foundation of Programs and IT Forums for Nigerian Youths is another solution that will help solve the problem of Internet fraud (Longe & Osofisan, 2011). Since the level of unemployment in the nation has contributed fundamentally to the spate of digital crimes in Nigeria, the administration ought to create jobs for

the youths and set up IT research facilities where these young people meet up and show their abilities (Olumide & Victor, 2010). This can be utilized genuinely towards creating IT as a part of Nigeria (Longe & Osofisan, 2011).

The other approach is to use an Address Verification System (AVS), which is a system that checks to guarantee that with the location entered on your request structure (for individuals that get orders from nations like the United States) coordinates the location where the cardholder's charging statements are sent (Olumide & Victor, 2010). Another approach is the development of Intelligent Voice Response (IVR) Terminals, which is an innovation that is designed to minimize chargeback and misrepresentation by gathering a “voice stamp” or voice approval and checking with the client before the dealer dispatches the request (Olumide & Victor, 2010). Another solution is the idea of tracking IP addresses, using software that could track the IP location of requests (Longe & Osofisan, 2011). This product could then be utilized to monitor whether IP location of a request is from the same nation incorporated into delivering addresses in the request (Olumide & Victor, 2010). Additionally, Nigeria can also use the video surveillance systems, which a consideration that human rights have supported in many nations (Olumide & Victor, 2010).

Finally, antivirus and antispyware software: Antivirus and anti-spyware programs are PC programs that PC projects that endeavor to recognize, upset, and wipe out PC infections and different pernicious programming (Anderson, et al. 2012). System firewalls might be equipment gadgets, programming programs, or a blend of the two (Anderson, et al. 2012). A system firewall ordinarily protects an inner PC system against noxious access from outside the system (Olumide & Victor, 2010).

Cryptography is the exploration of encoding and decoding data. Encryptions resemble sending a postal mail to another gathering with a lock code on the envelope, which is known just to the sender and the recipient (Olumide & Victor, 2010). Various cryptographic strategies have been created, and some of them have not yet been broken. Digital ethics and Cyber enactment laws are other approaches to the Internet fraud problem. Cyber morals and digital laws are likewise being defined to stop digital wrongdoings (Anderson, et al. 2012). It is an obligation of each person to take after digital morals and digital laws so that the expanding digital violations will lessen (Olumide & Victor, 2010). Security systems like antivirus software that are hostile to outside infections and spy products ought to be keeping in mind the end goal of remaining secure from digital violations. Web access providers likewise should be able to provide normal state of security at their servers with a specific end goal to keep their customers secured from a wide range of infections and pernicious projects (Salu, 2004, p. 161).

Chapter 3

RESEARCH METHODOLOGY

Introduction

The research method of the capstone is based on comparative design. The description is on worldview or philosophy, the underpinning practices and procedures for conducting and replicating research, and the type or research study. The paper will discuss the objectives of the intervention, how the intervention was developed, and how it will proceed. Then provide the supporting materials as necessary (agenda, handouts, and brochures, etcetera). Johnson (2008), stated that "data can be collected by qualitative data such as by open ended responses individual participants and observant." (p.14). this capstone will form the detailed step by step process of how the entire research study (the collection of data) was conducted. This will have to be where the implicit, explicit and observable sections of the research have been completed. The collection of comparative design data is a critical step in providing the information needed to answer the research question. This research includes the collection of some type of data whether it is from the literature or from subjects to answer the research question. The data can be collected in the form of words on a survey, with a questionnaire, through observations, or from the literature. Johnson stated that "data can be collected by qualitative data such as by open ended responses individual participants and observant." (Johnson 2008. p.14)

The data for this study was obtained partially from organizations and articles based on this topic. Some of it was obtained from the Internet Fraud Watch (IFW) yearly report projects. This organization works hand in hand with the National Consumers League's National Fraud Information Center based in Columbia (South America). They have carried out research and prepared reports on the top ten Internet scams, which included the "Nigeria 419 scam" that is very well known globally. This study examined reports dating from 1998 to 2002 (Anderson, et

al. 2012). It was done so because most of the Internet fraud reports or cases were never in the top list of 10 foremost Internet frauds. The research method employed a conceptual framework that perhaps "included the results of previous research on the same issue on the same issue and how it has affected the people of Nigeria" (Salu, 2004, p. 170).

Hypotheses Development: Dependent and Independent Variables

This research was based on two major variables: payment methods payment methods utilized while committing Internet fraud, and the demographic composition of the victims (Okonigene & Adekanle, 2009). This set of data composition was only available after 1998 when more information was in the hands of researchers as received from various reports. All the figures were in terms of percentage and were also categorized into the top 10 Internet scams (Anderson, et al. 2012). This was indicated by any given year, the type of swindle, and the degree and standing on a particular list. In most instances, a particular type of scam may not appear on the list following its one or two appearances, and emergent scams were also likely to appear year after year (Okonigene & Adekanle, 2009). From the period between 1996 through 2002 there existed roughly 19 Internet scams. Some were omitted because of their inconsistency, and there were only fifteen remaining.

Method of Data Analysis

Data was analyzed using a data set pertaining to the type of Internet scams and particular those that appeared on the top of the list (Anderson, et al. 2012). In the process of analyzing the data collected, the percentages were sorted and numerous scams sorted. "1" was assigned to the scam that had the highest prevalence level, and this was done from top-down the list (Okonigene & Adekanle, 2009). Conversely, "10" was assigned to the scam with the lowest level of prevalence. Secondly, the study also tabulated the number of occurrences on the top 10 lists

(Anderson, et al. 2012). Thirdly, the Internet fraud was found to have happened in all five years, based on the aggregate tabulated or computed. The main objective here was to identify the Internet scams that occurred mostly and are still being utilized by con artists in Nigeria (Anderson, et al. 2012).

The two variables mentioned earlier, which were payment methods utilized in the process of committing the crimes and the demographics of the people affected in the process, were examined utilizing the same two statistical measures; the standard deviation and arithmetic mean (Okonigene & Adekanle, 2009). Additionally, raw data was also presented in tabular form with the main of aim of examining the raw data set to determine the possible trends (Okonigene & Adekanle, 2009).

Chapter 4

RESEARCH FINDINGS

There are nineteen types of Internet tricks or extortion which were found among the seven main 10 postings from 1996 through 2002. Four of those tricks were no longer available on the main 10 postings after 1998, so they were expelled from further investigation (Okonigene & Adekanle, 2009, p. 3-9). They were (a) book deals, (b) club-enrollment or purchaser's club, (c) speculations, and (d) grant administrations. Every one of the four classifications made the postings just once. Except for book deals that made the top posting in 1997, the other three were not found on the main 10 postings again after 1996.

Fifteen types of online extortion were found for the period 1998 through 2014. Six of fifteen sorts of tricks seemed to make the main 10 records each year (Okonigene & Adekanle, 2009, p. 13). Put in another way, somewhere in the range of 40 percent of Internet tricks seemed, by all accounts, to be working exceptionally well, or were extremely prominent in light of the fact that they were reliably making the main 10 postings. Insights about the individual sorts of online extortion are exhibited in Table 1 and discussed hereunder:

i. Auction extortion initially showed up as the third most elevated class of online trick in 1997. Since 1998, it has reliably assumed the main position on the yearly postings.
ii. Like closeout fakes, the offer of general stock initially showed up in 1997 as the second most elevated sort of online trick. It has clutched this positioning from that point onward.
iii. In consecutive requests taking into account the normal positioning over the five years, the other four classes that have made the main 10 posting are (an) offer(s) of Internet administrations, (b) offers of PC hardware or programming, (c) work-at-home, and (d) advance charge advances (Okonigene & Adekanle, 2009, p. 15).

iv. One kind of new Internet trick merits consideration. The Nigerian cash offers made the main 10 posting in 2000 as the seventh most amazing positioned Internet trick. From that point forward, this classification has moved to the number three position in the last two years.

v. The main other paramount trick class is grown-up administrations. It has made the main 10 postings since 1999 and seems to have reliably positioned between the sixth and eighth most noteworthy kind of Internet trick (Okonigene & Adekanle, 2009, p. 15).

Category of Internet Fraud	Year					Year of Occurrences	Average	Overall Rank
	1998	1999	2000	2001	2002			
Adult Services	N/A	8	8	6	7	4		
Advance Fee Loans	9	6	5	8	9	5	7.40	6
Auctions	1	1	1	1	1	5	1.00	1
Business Opportunities	6	N/A	N/A	10	N/A	2		
Credit Card Offers	8	N/A	9	9	N/A	3		
Job Offer/Overseas Work	10	N/A	N/A	N/A	N/A	1		
Magazine Subscriptions	N/A	7	N/A	N/A	N/A	1		
Nigerian Money Offers	N/A	N/A	7	3	3	3		

Prizes, Charities, and Sweepstakes	N/A	N/A	N/A	N/A	10	1		
Pyramid Schemes/Multi-Level Marketing	7	10	N/A	N/A	N/A	2		
Sales of Computer Equipment/Software	3	4	6	4	5	5		
Sales of General Merchandise	2	2	2	2	2	5	4.20	4
Sales of Internet Services	4	3	3	5	5	5	2.00	2
Travel & Vacation	N/A	9	10	N/A	8	3	4.00	3
Work-at-Home	5	5	4	7	6	5	5.40	5

Table 1: Top 10 Internet fraud categories - 1998 through 2002

Category of Payment Method	1998	1999	2000	2001	2002	Average	Standard Deviation
Bank Debit	2%	1%	3%	5%	6%	3%	0.0207
Cash	3%	1%	3%	3%	2%	2%	0.0089

Cashier's Check	4%	5%	6%	4%	3%	4%	0.0114
Check	43	39%	30%	18%	14%	29%	o.1268
Credit Card	8%	5%	11%	29%	34%	17%	0.1316
Debit Card	0%	1%	2%	6%	7%	3%	0.0311
Money Order	38%	46%	43%	30%	30%	37%	0.0733
Telephone Bill	1%	1%	1%	0%	0%	1%	0.0055
Trade	0%	1%	1%	0%	0%	0%	0.0055
Wire Transfer	0%	0%	0%	3%	1%	1%	0.0130
Others	1%	0%	0%	2%	3%	1%	0.0130
Total	100%	100%	100%	100%	100%		

Table 1: Top 10 Internet fraud categories - 1998 through 2002

Online frauds were found to utilize around eleven sorts of payment techniques to propagate Internet wrongdoings (Okonigene & Adekanle, 2009). Utilizing the five-year medians, it was

found that there were three main techniques: cash request, checks, cash request, checks, and Visas. A few patterns merit additional discussion:

a) Even though checks have reliably been a top ten installment strategy for Internet tricks after 1998, their use has been diminishing (Okonigene & Adekanle, 2009). In 1998, somewhere in the range of 43 percent of the tricks included checks. By 2002, that figure had dropped to around 14 percent. Ultimately it has lost around 75 percent of its prevalence in the most recent five years (Okonigene & Adekanle, 2009).

b) Money orders, at one point, were utilized as part of around 46 percent of online misrepresentations, but they have now dropped to around 30 percent in the latest two years.

c) The credit card seems to have replaced checks and cash request as the quickest developing medium for propagating online extortion (Okonigene & Adekanle, 2009). Since 1999, its prevalence as measured utilizing the divided rate which seemed to have increased right around seven-fold.

d) Although their prevalence is currently lower, platinum bank cards and charge cards are two other installment techniques with an expanding pattern (Salu, 2004).

Age Category	1998	1999	2000	2001	2002	Average	Standard Deviation
Under 20	2%	3%	2%	4%	3%	3%	0.0084
20-29	16%	20%	20%	25%	21%	21%	0.0410
30-39	42%	30%	28%	28%	31%	31%	0.0610
40-49	24%	27%	29%	25%	26%	26%	0.0217

50-59	12%	15%	15%	13%	14%	14%	0.0130
60-69	3%	4%	5%	4%	4%	4%	0.0071
70 and Up	1%	1%	1%	1%	1%	1%	0.0000
Total	100%	100%	100%	100%	100%		

Table 3: Age distribution of Internet fraud victims - 1998 through 2002

It is evident that the IFW Project utilizes a sum of seven age bunches as the essential demographic criteria for following Internet extortion casualties (Okonigene & Adekanle, 2009, p. 14). Except for the first and the last classifications, whatever remains of the groups disappeared with age intervals of 10. As can be found in Table 3 above, there are four gatherings that indicated twofold digit rates. Utilizing the averages for the five-year time frame, the four gatherings represented around 92 % of all Internet misrepresentation casualties (Salu, 2004, p. 159). Around 78 % or one out of each eight casualties was from the 20 through 49 age group. The most noteworthy influenced bunch, around one out of each three casualties, was from the 30-39 age brackets. Two noteworthy perceptions about the information set are examined below: a) The 30-39 age brackets seemed to have leveled to around 28 percent, around one out of each three casualties, since 1999.

b) The 20-29 age brackets seemed to have grabbed the drop in rates from the 30-39 age brackets. In 1998, this gathering represented short of what one out of each five casualties reported. In 2002, this gathering developed to one out of each four casualties influenced.

c) The 40-49 and the 50-59 age bunch classes had all the earmarks of being the steadiest groups. On account of the previous, around one out of each four casualties was from this age bunch. On account of the last mentioned, they represented one out of each six casualties.

Chapter 5

CONCLUSION AND RECOMMENDATION

Conclusion

Looking at the data in chapter 4 of the research, online frauds were found to utilize around eleven sorts of payment techniques to propagate Internet wrongdoings (Okonigene & Adekanle, 2009). Utilizing the five-year medians, it was found that there were three main techniques: cash request, checks, cash request, checks, and Visas. (p.13)

As the all-inclusive community turns out to be progressively refined in their comprehension and utilization of PCs and as the advances connected with processing turn out to be all the more effective, there is a solid plausibility that digital wrongdoings will turn out to be more regular (Hastie & Dawes). Nigeria is evaluated as one of the nations with the most perhaps just "Internet fraud" or "cyber-crime."

Digital security must be tended to truly, as it is influencing the image of the nation as it is perceived by the outside world (Hastie & Dawes, 2001). A mix of sound specialized measures custom-made to the cause of Spam (the sending closes) in conjunction with lawful hindrances will be a decent beginning in the war against digital culprits (Salu, 2004, p. 162). Data assaults can be dispatched by anybody, from any place. "The aggressors can work without discovery for quite a long time and can continue to avoid any countermeasures." This for sure underscores the requirement for administration security offices to be aware of mechanical and security progressions (Salu, 2004). It will dependably be a losing fight if security experts are miles behind digital hoodlums (Hastie & Dawes, 2001). Battling cybercrime requires a comprehensive way to deal with this danger and all of its consequences (Hastie & Dawes, 2001). It is imperative to create a secured mindful society, including the general population, the ISPs, cybercafés,

government, security offices and web clients. Additionally, as far as procedure, it is essential to deliver issues identified with the requirement (Hastie & Dawes, 2001).

This Capstone is a research about some of the significant difficulties that Nigeria has been confronting for quite a while when it comes to cyber security issues. These difficulties are numerous; however, not every one of them was appropriately detailed and can be addressed without appropriate measures (Salu, 2004). At the same time, efforts are supported with the conceivable answers for capturing the difficulties. It is trusted that the circumstance of the nation will show signs of improvement if these arrangements are energetically put into place by both the legislature and subjects of Nigeria (Salu, 2004). Nigeria as a nation must fabricate it with consolidated exertion that will ensure that essential measures are implemented to curb the Internet fraud problem (Hastie & Dawes, 2001).

Theoretical Implication of the Study

This study utilizes openly accessible NFIC (Nigeria Financial Intelligence Center) information sets covering the period of 1998 through 2002 specifically; this study found that there are definite patterns and perceptions about online frauds, particularly in Nigeria. Initially, six types of Internet frauds were relied upon during the main 10 yearly listings (Salu, A.O., 2004, p. 160). Amid the period examined, the internet trades and offers of general stock were the two most well-known tricks utilized by online swindlers (Hastie & Dawes, 2001). The Nigerian cash offers that have appeared on the main 10 list only three years back is one online trick class that ought to be monitored closely to ensure that such cases are curbed. In any given year, certain new tricks may likewise show up, and existing ones may simply drop off the rundown (Hastie & Dawes, 2001). Be that as it may, the six online fakes that have made the postings each of the five years are relied upon to keep going for some time (Hastie & Dawes, 2001, p. 284).

Secondly, the three most prominent strategies for installment utilized as part of Internet extortion are checks, cash requests, and charge cards (Hastie & Dawes, 2001). Checks are declining in prevalence as an extortion medium. Then again, Credit cards, are demonstrating an unfaltering increment as a medium for online tricks (Hastie & Dawes, 2001). Despite the fact that relatively few cases involved just charge just charge cards and bank charges, both of these mediums demonstrated a moderate yet continuous expansion (Hastie & Dawes, 2001).

Finally, in light of the age brackets utilized by the NFIC, casualties of Internet extortion can be entirely different. They go from those in the under 20 age brackets to those that are over 70 age brackets. Be that as it may, somewhere in the range of 92 percent of the casualties are inside the 20 to the 59 age brackets. More than 50 percent of the casualties are from the 20 to 39 age brackets (Hastie & Dawes, 2001, p. 285).

All the significant patterns indicated in this dissertation demonstrate that registering teachers can minimize Internet extortion in an assortment of ways. Many youths are not educated and they move around seeking ways of ensuring that they make a living, and that makes them vulnerable to Internet crimes. Above all else, one of every two casualties of Internet extortion is from two noteworthy age groups or brackets going to school (Hastie & Dawes, 2001). In a typical college or university setting, the vast majority of the customary students are in the 20-29 age brackets, while the non-conventional students are in the 30-39 age bracket (Hastie & Dawes, 2001).

Computing teachers can make a noteworthy commitment to the battle against Internet misrepresentation by instructing these two sets of students about legitimate web shopping conduct (Hastie & Dawes, 2001). When students and other unsuspecting victims are educated regarding the challenges and ways of handling online transactions, it becomes easy to address the

problem wholesomely. Perfect courses for covering this material may include PC proficiency course in the general studies center, courses on data frameworks, standards course or an earlier software engineering course (Hastie & Dawes, 2001). With some understanding of what and how online extortion is sustained on the Internet, understudies will, at any rate, recognize what to keep an eye out for when shopping on the Net.

Second, instructing understudies about “good and bad” choices and the educating of morals ought to be incorporated into a course in the undergrad general main subjects (Hastie & Dawes, 2001). Progressively, colleges have evaded far from the instructing of appropriate, direct and character building in light of the fact that regularly it includes the exchange about religion and quality frameworks. Without a solid conviction, a profoundly capable and innovation keen graduate may turn into a risk to society by taking part in online misrepresentation (Hastie & Dawes, 2001, p. 286). A course in morals can give the required training to an understudy for good performance in the activities which are worthy of their impediments. Third, processing instructors can likewise minimize Internet extortion issue by creating and planning courses on e-business security frameworks (Hastie & Dawes, 2001). A portion of the innovations that have been incorporated into late course content incorporates open key framework, computerized testament and validation, data certification, frameworks resistance, and Web content examination. Understudies who have taken courses in such front-line innovations will be able to fabricate more secure PC frameworks (Hastie & Dawes, 2001, p. 286).

Finally, Internet researchers can now have a greater effect in the battle against Internet extortion by giving the required authority to make multi-disciplinary decisions that can convey secured frameworks for the long term (Hastie & Dawes, 2001). For instance, such teachers can collaborate with money and bookkeeping instructors to distinguish potential payment

frameworks that contain some type of insight for activating ongoing misrepresentation notices. A conceivable region for such research financing may originate from saving money industry in light of the fact that a mind-boggling measure of the extortion is conferred by means of the electronic cash clearing framework (Hastie & Dawes, 2001). Endeavors toward the end of minimization cash misfortunes ought to hold any importance with managing the banking sector.

This thesis finds vital reason to continue investigating this issue that has affected Nigerians for quite a while because there are numerous frauds that will likely transpose to the Internet (Hastie & Dawes, 2001). This is probably because numerous categories of frauds are already conceptually transposed to the Internet and the level of frauds being perpetrated on the Internet today. These are challenges that have always affected other nations too, and it will be essential to further research additional concrete solutions (Hastie & Dawes, 2001, p. 287). It will be necessary that legal measures and the government put a committed fight against Internet fraud. It is noteworthy that each single measure presented in this research should in the future be considered as proposals for further research. They will only help to develop emergent countermeasures against e-fraud.

It is evident that cyber security is a reality that must be managed now, as it has the potential to determine how Nigeria is viewed globally. Today's reality is an imperative advancement, such that physical exchanges in all circles of ordinary life will be done online, from bank transactions to controlling many of the systems that we operate on a daily basis. This way, there is a requirement for digital exercises control that sheltered gatekeepers for Nigerians who are inside as well as the outsiders who are intrigued by putting resources into Nigeria.

Cybercrime with its complexities has proved to be difficult to defeat. Amplifying the guideline of law into the Internet is a basic stride towards making a reliable situation for

individuals and organizations. Since the procurement of such laws to adequately dissuade cybercrime is still a work in progress, it gets to be necessary for people, associations, and government to design methods for giving security to their frameworks and information. To give this self-assurance, people, associations, and government ought to concentrate on executing cyber security by arranging, tending to individual's procedure and innovation issues. Then more assets should be placed for instructions and mindfulness on security practices.

According to BBC (2016), "A Nigerian behind thousands of online scams around the world has been arrested in the southern oil city of Port Harcourt, Interpol alleges. The report also stated that the 40-year-old man, known only as Mike is alleged to head a network of 40 individuals behind global scams worth more than $60m (£45m). His operations involved using malware to take over systems to compromise emails, as well as romance scams. Nigeria's anti-fraud agency was involved in the arrest" (para. 1-3)

In this manner, there is no single measure that will cure the danger of Internet fraud and guarantee cyber security. In any case, it is the blend of measures together with the genuineness and meticulousness with which they are executed and administered that will serve to diminish hazards most successfully and productively. Likewise, the battle against Internet fraud and cyber security dangers in Nigeria requires that people should learn about Information Technology as well as Information Technology intelligence to help curb the increasing cases of Internet frauds in Nigeria.

References

Adebusuyi, A. (2008). The Internet and Emergence of Yahoo boys sub-Culture in Nigeria, International Journal of Cyber-Criminology, 0794-2891, Vol. 2(2) 368-381.

Amaka E, (1995), THISDAY is published by Thursday Newspapers LTD. Retrieved July 15th, 2016. www.thisdaylive.com

Anderson, R., et al. (2012). Measuring the cost of cybercrime, 11th Workshop on the Economics of Information Security (June 2012), Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Augustine, C.O., MIEEE (2010). Cybercrime & Cert: Issues & Probable Policies for Nigeria, DBI Presentation, Nov 1-2.

Hastie, R. & Dawes, R.M. (2001). *Rational Choice in an Uncertain World* (2nd ed.) illustrated New York: Sage Publications.

Johnson, B., & Christensen, L. (2008). Educational research: Quantitative, qualitative, and mixed approaches (p. 34). Thousand Oaks, CA: Sage Publications

Laura, A. (1995). "*Cyber Crime and National Security*: The Role of the Penal and Procedural Law," Research Fellow, Nigerian Institute of Advanced Legal Studies. Retrieved from http://nials-nigeria.org/pub/lauraani.pdf

Longe, O., & Osofisan, A. (2011). *African Journal of Information Systems.* 2011, Vol. 3 Issue 1, preceding p17-26. 11p.

Oghenerukevbe, E.A. (2008). Customers Perception of Security Indicators in Online Banking Sites in Nigeria. *Journal of* Internet *Banking & Commerce.* Dec2008, Vol. 13 Issue 3, Special Section p1-14. 14p.

Okonigene, R. E., & Adekanle, B. (2009). Cybercrime in Nigeria, Business Intelligence Journal, Retrieved from http://www.saycocorporativo.com/saycoUK/BIJ/journal/Vol3No1/Article_7.pdf

Olumide, O. O., & Victor, F. B. (2010). E-Crime in Nigeria: Trends, Tricks, and Treatment. *The Pacific Journal of Science and Technology,* Volume 11. Number 1.

Salu, A.O. (2004). Online Crimes and Advance Fee Fraud in Nigeria -- Are Available Legal Remedies Adequate? *Journal of Money Laundering Control.* Dec2004, Vol. 8 Issue 2, p159-167. 9p.

Strassmann, P. A. (2009). Cyber Security for the Department of Defense, Retrieved July 10, 2011, from http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf

Taylor, R., Fritsch, E., & Lieder Bach, J. & Holt, T. (2015). Digital crime and digital terrorism *(3rd Ed).* Upper Saddle River, N.J.: Pearson. *www.bbc.com/news/world-africa."*Top Nigerian scammer arrested*".* Retrieved August 1st, 2016.

www.cybercrime.gov.ng