Cydpan Research Journals
International Journal of Social Sciences and Economic Development (IJSSED)
Volume 1, Number 1, June 2023
ISSN: 3026-9024
https://cydpanjournals.com/

Youths and Internet Fraud in Nigeria: X-raying the Impact of Digital Age of Human Security

Onwunyi, Ugochukwu Mmaduabuchi
Department of Political Science,
Dennis Osadebey University, Anwai Road, Asaba
Email: ugochukwu.onwunyi@gmail.com

ABSTRACT
The menace of internet fraud has eaten deep into the fabrics of our society and poses threats to the socio-economic development of the country. It is pertinent to state here that although internet fraud is a global phenomenon, the vulnerabilities and impact trends do tend to differ depending on the strength of the measures each country put in place to combat menace such as cyber laws and cyber protection technologies. Sadly, as shown in the arguments above, Nigeria ranks high amongst the internet fraud impacted countries however the country's response to mitigate internet fraud is still very low due to inadequate internet fraud legislations, limited technology and lack of cyber security experts. The shortage of human capital in cyber-security hence becomes a major vulnerability factor in addressing Nigeria's security needs to combat internet fraud and cyber threats emanating from cyber criminals. This paper is qualitative in nature as data collection was based on the secondary sources of data, while the society risk theory formed that analytic framework. Following these submissions, the paper concludes that efforts by the government and the citizenry geared towards curbing internet frauds must be reinvigorated as cyber security is crucial for maintaining the continuity of vital social services, preservation of public trust in information systems and promotion of socio-economic development in Nigeria. Following the conclusion reached in this study, the following recommendations have been proffered; the government should pursue aggressive public sensitization against internet fraud using the mass media and the promotion of personal cyber space security should be incorporated in the primary, secondary and tertiary education curriculum; individuals need to observe simple personal safety rules such as not disclosing to strangers personal effects and banking details such as credit card pins, bank account numbers, e-mail codes and use of antivirus on their systems against malware etcetera.

Keywords: Internet, Fraud, Human Security, Digital Age, Nigeria

INTRODUCTION
Cyber technology has transformed virtually all human activities including we communicate, travel, power our homes, run our economy, and obtain government services. Despite how many benefits that is associated with improved cyber technology, there have equally being some major disadvantages associated with it; one of them which is internet fraud. As human activities become more dependent on technology, it equally poses serious threat to people's lives and properties.

The spate of cyber criminality has become a disturbing phenomenon in Nigeria as individuals report cases of scam text messages about winning 'promos' and scam emails on tempting and attractive business proposals (State CID, 2012) A typical example of such scam text message sent to a nonacademic staff of the Department of Sociology, University of Calabar, Calabar on the 2nd of October, 2012 read as follows, "Your cell number has been awarded $315,000 in the ongoing Nokia UK promo, for claims send your name, account number and country to claimsukpro2012@hotmail.com". Many may have fallen victims to such scams. The frequent occurrence of these cases and how people fall victims instigated the quest to find out if becoming a victim of internet fraud or not depends on the level of awareness on internet fraud activities. Aghatise (2006), Adalemo (1999), Adomi and Igun (2008) and Adeniyi (1999) were all of the opinion that youths are the 'base fabric' for future growth and sustainable development of a nation, they represent the foot soldiers for social change, economic development and technological innovations. Hence, the ineptitude of leaders in Nigeria to promote positive values for youths is often translated into social incongruence (Adeniyi, 1999). This implies that youths who are not well taken care of get involved in the perpetration of criminality, which includes cyber criminality. As true as these assertions may sound, they could not establish a link between youth and cyber criminality, and did not also ascertain whether youths are the major perpetrators of internet frauds in Nigeria, or Calabar in particular.

Adeniran (2006) also opines that the proliferation of youth's online fraudulent practices is strongly connected to societal emphasis on materialism and wealth accumulation. But he did not provide supportive or comparative data linking youth to these crimes. Technological advancements are supposed to provide the youth opportunities for growth, learning, skills development and expansion of their knowledge base. However, in recent time, technology has be abused and used for criminal activities which mostly occur through internet fraud activities. This trend has had a global touch in recent time, with the most occurrence been observed among youths in developing nations like Nigeria. It has been argued and documented in various official documents that Nigeria is the hallmark of internet frauds. As a consequence, the attention of the government, religious institutions and other concerned security agencies has been drawn into devising measures and policies that could ameliorate this trend.

Methodology and Theoretical Framework

The research adopted qualitative method of research involving data collection from secondary sources and content analysis. The study however relied on the consultations of textbooks, journal articles, newspaper, magazines, internet

materials, e-library etc. The critical descriptive method of analysis was also used to compliment the triangulation of the sources of data for the study.

Theoretical Framework of Analysis

This study adopted the Risk Society Theory as the analytic framework. This anchored on the theoretical underpinnings of German Sociologist, Ulrich Beck"s "*risk society theory*". The theory holds that there is a movement away from traditional and industrial society and towards a new modern "*risk society*" which is individual, global and self-confrontational (reflexive). Beck (1992:21) defines the risk society as "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself". The nature of modern societies is such that risks multiply with the increasing "complexities" of societal systems of production, consumption, governance and technological control and as Jonathan, Nick and George (2004) posits, high modernity is characterized by the production and distribution of risks from an increasingly complex techno-scientific system. Similarly, Bell (1998 cited in King and McCarty, 2009) describes risk society as "a society in which the central political conflicts are not class struggles over the distribution of money and resources but instead non-class-based struggles over the distribution of technological risk". Hence, the risk society is one where every citizen is exposed, to some degree, to technological dangers such as radioactivity, airborne and waterborne pollution, and hazards from mass transportation such as airline, automobile or train crashes, including internet frauds. This implies that paradoxically scientific and technological advancement produces new forms unintended risks and does portend severe consequences for society. Beck (1992) rightly demonstrated this when he asserts that in late modern society risk is increasing due to technology and science rather than being abated by technological progress and it is not a world which is less prone to risk, but it is "*world risk society*" with magnitude of risk so great, that transcends both time and place, by becoming global in scope, the control of risk across is both impossible and meaningless.

The risk society theory is so apt with the advent of the internet revolution and mobile telephony technology which has aided instant messaging, communications, electronic business transactions, banking, and electronic learning anywhere in the world just by the click of a mouse. The globalization process is fast tracked with the information communication technology as hitherto distance and space barriers between countries are no more with the world shrinking into one global community. Hence, the positive role of the internet technology revolution on the development of the society cannot be overemphasized, however like every other technological innovation it came with it unintended risks which

includes internet fraud. The internet hosts billions of computers with billions of people behind those computers and one is unaware of the risk that can occur with a single click of mouse as hacking, fraud and online schemes are some of the risks to which internet users are exposed to. The "*Information Society*" we live in today thus creates unintended risks such as property theft, money laundering, terrorism and so on that are mostly virtual, invisible and most likely irreversible thereby exhibiting a "*Risk Society*" for individuals, organizations and governments with severe implications for technological and socio-economic development.

Literature Review

Internet Fraud and Youth Defined

According to Maitanmi and Ayinde (2013) internet fraud is a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Similarly, Okeshola (2013) opined that the term internet fraud can be used to describe any criminal activity which involves the use of computer or the internet network, including such crimes as fraud, theft, blackmail, forgery, and embezzlement. Youth is best understood as a period of transition from the dependence of childhood to adulthood's independence. That's why, as a category, youth is more fluid than other fixed age-groups. Yet, age is the easiest way to define this group, particularly in relation to education and employment, because 'youth' is often referred to a person between the ages of leaving compulsory education, and finding their first job. The United Nations, for statistical purposes, defines 'youth', as those persons between the ages of 15 and 24 years, without prejudice to other definitions by Member States. The Secretary-General first referred to the current definition of youth in 1981 in his report to the General Assembly on International Youth Year (A/36/215, para. 8 of the annex) and endorsed it in ensuing reports (A/40/256, para. 19 of the annex). However, in both the reports, the Secretary-General also recognized that, apart from that statistical definition, the meaning of the term 'youth' varies in different societies around the world. When the General Assembly, by its resolution 50/81 in 1995, adopted the World Programme of Action for Youth to the Year 2000 and beyond, it reiterated that the United Nations defined youth as the age cohort of 15-24 (Onwunyi & Okonkwo, 2021).

Factors that influence Youths to the Engagement in Internet Fraud

Urbanization is one of the causes of internet fraud in Nigeria; it is the massive movement of people from rural settlement to city. Urbanization is looked at as the massive physical growth of urban areas as a result of rural migration in search for a better life. This result in a heavy competition amongst the growing populace

more especially the youths, as such the youths find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest. Nana (2015) in a study in Ayawaso East Constituency of the Greater Accra Region using a sample of 100 youths who are internet fraud culprits found that 47.5% of respondents were from the Northern region which is basically the urban area while only 5% were from the typically rural region. Also, Elgbadon and Adejuwon (2015) in a study in Lagos and Ibadan aimed at finding out factors that predict engagement in cyber-crime among young people, using 986 young people found that urbanization was specifically mentioned by the youth as the major cause of internet fraud. Another study by Abia et al (2010) in Bamenda region of Cameroon using 386 students found that scamming was common in the urban areas than in the rural areas.

Unemployment

In Nigeria, the unemployment rate is worrisome. It has consistently increased in the last few years. Unemployed youths are readily available for anti-social criminal activities that undermine the stability of society. Umeozulu (2012) in a research on causes and perception of internet fraud in Caritas University in Enugu found that unemployment is the major determinant of cyber-crime. Also, Femi, Dada and Ayibaabi, (2015) in their study on perceptions of impact of unemployment on crime in Landmark University students found out that 83.19% of the respondents perceived that youths are involved in crime as result of unemployment. Another study by Tade and Aliyu (2011) on the determinant of internet fraud among undergraduates of University of Ibadan identified as "yahoo boys" reported one of them as saying "the unemployment rate in the country is so degenerative that, if you are not wise, you will become useless in this country. The means of survival is through being creative".

Quest for wealth

Another cause of internet fraud in Nigeria is quest for wealth. In their research carried out in Ogun, Oyo and Lagos states Muraina and Muriana (2015) found that, there exists a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Most internet fraud requires less investment and a conducive environment. Nigeria is such an environment and many cyber criminals take advantage of that. In another related study, Ndubueze, Igbo, and Okoye, (2013) in Lagos found out that many young people in Nigeria spend all day in the internet not only due to high rate of unemployment but also as a result of get rich quick syndrome which they feel can happen through the internet. The over-emphasis on

wealth by the Nigerian society has left the youth with no other choice but to pursue it, albeit by hook or crook. Internet fraud, with its anonymity, speed and relative guarantee of returns, has become pretty fashionable among the youth. With poor recreational facilities, most youths have found a recreational haven of some sort in cyber cafes where they hang out for the better part of their day.

Peer Pressure

Peer group with shared experience are an inevitable source of personal relationships. Existing crimes that have been transformed in scale or form by use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale; the frequent interactions with peers, particularly with deviant peers sometimes lead to the adoption of antisocial behaviour for group conformity. Young people need to formulate a new identity and to establish autonomy from their parents. The frequent interaction with peers, even more frequent than with parents, can lead to peers becoming the primary basis for social comparison. Ibrahim (2016) did a qualitative study to explore the experiences and perceptions of 17 parents (10 males and 7 females) of Nigerian descent living in England who have a mean age of 45 years. Findings show that all the participants reported that peer pressure is the most important factor that lure Nigerian children's involvement in internet frauds.Another study by Okeshola and Adeta (2013) in Zaria on factors that lead undergraduates to internet fraud, found out that majority of respondents 86% opined that peer group is the cause of internet fraud in Zaria, Kaduna state of Nigeria. In another related study, Holt (2011) in a Kentucky school district in United States of America. Study results showed that the biggest predictor that youths might engage in internet fraud is peer influence. He also observed that low self-control has both a direct and indirect effect, through other peers offending, on youth internet fraud. The study notes that both low self-control and deviant peer associations have been linked, not only to internet fraud violations, but also to committing other crimes. They also found that peer offending had a stronger effect on others offending than low self-control and also consistently predicted each type of cyber deviance. In the study, it was noted that internet frauds may be more attractive to youths than real world offenses because of the relative anonymity that the internet and computers provide their users.

Internet Fraud and Social Media

Internet and social media has been implicated in the rise of cyber-crime among youths. Shabnam, Faruk and Kamruzzaman, (2016) carried out a descriptive type of cross sectional study in Tangail municipality and Dhaka north City Corporation areas in Bangladesh. The aim was to assess the perception, causes and consequence of cyber-crime among youth using purposive sampling method taking a sum of

118 respondents. The study found that social media encourages dissemination of false information and that most people who visit the internet are vulnerable to internet fraud. Also, Saridakis, et al., (2015) in a study of the relationship between online victimisation and users' activity and perceptions of personal information security on social networking services (SNS) using 514 internet users found that social media users with high-risk propensity are more likely to become victims of internet fraud, whereas those with high perceptions of their ability to control information shared on SNS are less likely to become victims on social media. Sex of young people has also been addressed by scholars as a big factor associated with internet fraud. Kamruzzaman et al, (2016) in a study, found that male students are more likely to engage in internet fraud than females and that most of the respondents who are involved in internet fraud do just for mere interest and not for the illegal monetary gain. Another study by Choi, Choo and Sung (2016) on risk factor in computer crimes using 204 respondents in Japan found that males are more likely to be engaging in online risky leisure activities such as visiting unknown Web sites, downloading free games, free music, and free movies than females. Also, Elgbadon and Adejuwon (2015) in a study in Lagos and Ibadan aimed at finding out factors that predict engagement in internet fraud among young using 986 young people found that males are more likely to engage in internet fraud than females.

Youths and Internet Fraud: The Nexus

There are different opinions about what should constitute a youthful population in Nigeria, and the age bracket to be considered as being youthful. Though, the Social Development Policy for Nigeria in 1980 asserts that a youthful population should fall between 12 to 30 years of age. For this study, a youthful population is considered as young Nigerians who fall between the age bracket of 18 and 40years. However, this contention in definition or determining who is a youth and who is not, does not extend to the attributes or characteristics possessed by Nigerian youths. Nigerian youths are daring, adventurous, industrious, diligent and hardworking, (Adalemo, 1999). In fact, if properly gingered or spurred up, Nigeria youths are capable of working tirelessly for the development of their immediate society, (Mabogunje, 1999). For Adeniyi (1999), youths are the foot soldiers for the improvement and development of any given society. He sees youths as the front burner of any form of societal change, technological innovation and development.

Therefore, the ineptitude of leadership and government in Nigeria to cultivate good moral standards and necessary societal values amongst youths has made them to imbibe moral decadence and negative values such as cyber criminality.

Youths in Nigeria are being pushed to the wall with the bane of corruption, unemployment and poverty making them to find succour in crime. Every society has a dominant set goal that every citizen strife to achieve. In the case of Nigeria, this dominant goal is perhaps massive wealth accumulation. Hence, Merton (1938), when the institutionalized means of achieving these societal set goals is open to just a few, others device different modes of adaptation which result to crime situation. It therefore follows constructively, that youths in Nigeria whose opportunities of accumulating material wealth are blocked by the bourgeoning Nigeria class have resorted to cyber criminality to make ends meet. Also in Nigeria, questions are not usually asked about individual's sudden wealth, let alone public officials giving account of their stewardship. Therefore, youths in the face of this moral decadence and corruption have decided to eschew good morals and embraced cyber criminality. According to Ninalowo (2004), great inequalities exist in Nigeria. The gap between the rich and the poor is widening every day. Even the ill-gotten bourgeois have unflinching societal affluence and the society does not react to how their wealth was gotten. He posits that, in this kind of society, the poor youths will reject rules and norms governing the society to embrace criminality which include internet frauds. This is evident in the activities of the yahoo boy's sub-culture. Their scam activities have given Nigeria a bleak image across the globe, and millions of naira have been lost to cyber criminals. Young Nigerians have been caught with huge amount of monies in their bank accounts, (www.efccnigeria.org). This ill-gotten wealth is nothing but a poison to the Nigerian economy. The Nigerian youths are at a cross road, and if nothing is done to stem the tide of cyber criminality, then Nigeria could be sitting on a time bomb, and it may detonate in the form of a revolution as predicted by some world super powers and book markers.

Empirical Review

What makes cyber criminals in Nigeria look mystical to people within and around the world is the innovative approach engaged in their operations. They devise numerous ways to beat the imagination of the victims and as security agents discover one of their antics, another one is invented over and over, again and again. Researchers have shown that many operations are professionally organized in Nigeria (Ogwezzy, 2012). In most occasions, when potential victims makes attempt to carry out a thorough background check on the proposed business from scammers, they often found out that everything is appealing to common sense. This makes them to believe that the business is genuine. Thus, wealthy foreign investors, medium and even small scale businesses including private individuals are duped millions and billions of dollars and other currencies. Only in few instances that such background checks would yield positive result for them to discover that

the proposed business is a scam and withdraws from the communication link immediately. This success is usually achievable when the fraudsters are in a less organised gang, because a well organised gang always fix every piece together. For Ani (2011), the ICT-induced tactics employed by cyber criminals include but not limited to the following; the use of fake cheques, Western Union/Money Gram Wire Transfer, Anonymous Communication, web based email, bad English, email hijacking/friend scam, Short Message Service (SMS), fake websites, invitation to visit a country, purchasing goods and services, vehicle matching service scams, cheque cashing, lottery scam, charity scam, fraud recovery scam, bona vacantia, fake job offers, rental scams, etc.

According to Ige (2008) and Adomi (2008), wire transfer via Western Union and Money Gram is often used by cyber criminals because the transaction between the perpetrator and the victim is not traceable and cannot be reversed. The composition in Western Union is that, once the money is sent, both the source and the destination are concealed against a third party and can never be cancelled. Other means of transferring cash without revealing the sender and the receiver are postal money orders and cashier's checks. Since these routes of wire transfer hide the true identity of internet fraudsters, it is often used to wreak havoc on their targets or victims. The following options have been identified by Adebusuyi and Adeniran (2008) as tactics widely used by cyber criminals. One of the modus operandi of cyber criminals operation is the use of "Bad English". Scammers deliberately fill the content of their communication with faulty grammar and wrong spellings. This gimmick enables the potential victim (who may be very educated and fluent in English) to think that he or she cannot be fooled by an illiterate person. Most times, even when they know that the message or information is a scam, they still go ahead to respond and follow up the deals with a false thought of superiority over the scammer, until they are ripped of valuables, money and personal belongings.

Web based e-mails is another method of communication used by cyber criminals because it does not allow for valid identification of information sent to a particular victim. In fact, some of these mails services conceals the sender's IP address very well, making it possible for a cybercriminal to hide his or her identity up to the country of origin. Agboola (2006) discovered that, because of the diversity of the internet, a cybercriminal can have numerous e-mails account at a particular point in time, and apart from that, they can engage in email hijacking and friend scam involving the hijacking of people's e-mails, and use them to obtain by false pretense. This is usually done by phishing, key logger or computer viruses in order to have login access to people's emails accounts. A transaction may have been

initiated using a yahoo software but could be completed using a fax machine, whenever their victim request for physical documents. Also, in making sure that they are not traceable at all, cyber criminals use prepaid mobile phones linked to a personal mobile or public fax For Basil (2007), internet frauds are not executed using the methods enhanced by e-mails alone. Most of them diversify their acts with the use of "charm websites". Charm is an African metaphysical power used to act against a sane point of reasoning on the part of victims. These charm websites are created as sham or a decoy in semblance of a true website, for instance, smart gov.cr.ng, Central Bank of Nigeria, Unical.edu.ng, etc. Some are created to look like non-existing organisations or parastatals in order to give the fraudster creditability.

In the work of Ayoku (2005), there is a different method involve, where actual or legitimate activities of a company are captured to make it look real in order to build confidence and trust from potential victims, and eventually dupe them. Furthermore, following an advanced stage of cyber criminality, some victims are lured to a town, state or any location to meet a perpetrator who has professed good intentions during the process of communication, then they are kidnapped for a ransom or sometimes killed like the famous story of Cynthia Osokogu who was killed by her Facebook assailant on July 2012 in Lagos State. The criminals usually provide Visa or transport as the case may be. A cybercriminal having successfully duped a victim, recognizes that, the same victim may fall fast in another scam than a potential or a new one, (Akinola, 2006). This is done by reaching out to the victim who has just been duped pretending to be a police officer. Informing the victim that some fraudsters are in the police net, and having heard about his predicament, everything that was stolen from him or her has been recovered. At this point, the success of scamming the victim again is guaranteed because he or she sees the police officer as a third party yet knows much about what was stolen. It is this false thought that will guarantee the release of more money when asked to pay for the retrieval of his or her lost items. Only to discover that it is a follow up scam when these items are never released.

Others use telephone calls or Short Message Service (SMS) to random victims, sometimes call their names and create familiarity. This method of operation is common in Calabar Metropolis. Victims are usually given attractive business proposals such as the supply of Solar Panels or winning promo alerts etc. In September, 2011, an SMS was revolving around Calabar Metropolis and other parts of the country, advising loved ones not to pick calls from a certain number (010911), else they will die. This was just a scam SMS to make millions of naira from GSM subscribers. The scammer buys bulk SMS from any of the service

providers (MTN, GLO, AIRTEL or ETISALAT) and open a domiciliary account so that all charges on the messages drops into the account. Nigeria has a population of approximately 167million (National Population Commission, 2011), assuming 15million people circulate this SMS at the cost of N5 per message, you can imagine the millions. Meanwhile, the scammer had just used a date of 1st September, 2011 (010911) to exonerate himself from legal implications.

In 2009, youths in Calabar Metropolis went haywire looking for old pendulum clocks. Cyber criminals offered N500, 000.00 for mercury usually found in the clock. It was speculated that this mercury malfunctions the Automated Teller Machine (ATM). This situation provided a real scare as youths could do anything humanly possible to have this money, until the State Government had to put a stop to the search of these "Abrahamic Clocks". Computers and GSM phone dealers buy viruses online, and circulate same to infect these equipment's. This is to make money from the sales of anti-viruses. Some of the viruses we have in circulation in Calabar Metropolis are Comb Warrior and Caribea (Phonesolution, 2005).

According to Microsoft Company (2011), most newly acquired computers in Calabar and other parts of Nigeria are usually installed with pirated Windows. This can be affirmed as we see Laptops, notebooks and desktops owners pay meager amount to dealers for installation of their systems ignoring getting the original version direct from Microsoft online. Also, cyber prostitution and child pornography has become the order of the day in Calabar Metropolis and Nigeria as a whole, through social networks such as facebook, 2go, Skype, WhatsApp and blackberry pinging. The young generation has seized the opportunity of these social networks to corrupt the moral fabric of our society in terms of prostitution, pornography, cyber theft, cyber stalking and scamming. The activities of cybercriminals are having a tremendous effect on our society as a whole. Internet frauds has cost the whole world a fortune, (Oludayo & Ibrahim, 2011). It is actually difficult to state clearly or categorically, how much has been lost to internet frauds, because most of these crimes are insiders' jobs and are left unreported. According to Ultrascan Advanced Global Investigation (2007), Nigeria is losing about $80million yearly to internet frauds. Also, the American National Fraud Information Center in 2012 reported that Nigeria money scam has grown up to about ninety percent of perpetration. The center also predicted that Nigeria internet frauds are skyrocketing to a worst height in the nearest decade. For Katyal (2003), internet fraud is a canker worm that is eating deep and retrogressing the economy of nations, because in every year, millions and billions of dollars are being lost to internet frauds across the world.

Following Katyal perception, the world's population is estimated at 7billion people, assuming a paltry 3billion people are ICT compliance, doing businesses, exchanging ideas and innovation on the internet, you can imagine how much will be lost if cyber criminals preys on them. According to Tunji Ogunleye, a member of Nigeria Internet fraud Working Group (NCWG), the negative uses of the internet by fraudsters in Nigeria outweigh the positive usage. He expresses shock that out of the 60th countries that embraced ICT, Nigeria is the 56th country, yet ranked third among the top ten countries of the world in internet fraud perpetration. Ogwezzy (2012), also noted that, the damage cause by internet frauds to the Nigerian economy is escalating day and night. He further predicted that internet frauds if not curb, will have severe economic and financial impact on the Nigerian society. For Abubaker (2009), because of internet frauds, Nigeria financial documents such as bank cheques and drafts are now being viewed with suspicion in other countries of the world. This means that our financial documents are no longer viable and reliable pieces for international transactions. Also, Nigeria e-mails no matter how legitimate are now being blacklisted by the international community. Even internet communication waves from Nigeria are being blocked by other countries internet gateways. Nigerians are now being generally discriminated upon in the world because of the "yahoo boys" syndrome. According to Chawki (2009), International Banks now do proper findings and protracted researches on Nigeria financial transactions before clearance often causing delay. For this reason, foreign investors are scared of ploughing their huge capital into Nigerian economy by way of investing.

Internet Fraud and Human Security in Nigeria

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritate by the question, *'Why there is too much ado about crime?'* No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behavior! However, it should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to the society. In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes. Conceptually, crime is a dynamic and relative phenomenon and subjected to the relative socio-political & economic changes occurring in existing system of society. Therefore, neither all-time suitable comprehensive definition encompassing all aspects of 'crime' is possible at any moment of time nor can a

single definition be made applicable to different society. With its dynamicity, it is influenced by the changes occurring in the correlated phenomenon and value system generated by these changes. As evident in present scenario where money is more valuable than values, a definite hike in the corruption related offences are observed where social morality is low which influence the commission of crime attached less social stigma than ever before. Incidentally economic crime is on its peak. This clearly reflects that crime has its interdependency with other social phenomenon, economic systems and political machineries. Also, the population is one of the important factors influencing incidences of crimes. A positive correlation between the growth in incidences of crime and the population of the country has been observed. Besides population, the other factors influencing the crime are such as situation at a particular place, rate of urbanization, migration of population from neighboring places, unemployment, income inequality, [computer literacy in case of Cybercrime] etc. At the same time, the economic structure of give society is also influence the economic crimes. As every controlling systems for crime has much to do with the political system which prescribe norms, make rules, create preventive measure, the political structure and system also influence the crime in given society. This clearly demonstrates that every definition of crime has correlation with the socio-economic and political factors.

These days a worst fear in teenager's eyes is Cyber Bullying. It is become common over past five years, generally from the age below eighteen are more susceptible and feared from Cyber Bullying as per inspection. It is becoming an alarming trend in our society. As per inspection of data, the worst fear of cybercrime is on teenagers female. Cyber Bullying is a fear when person receives threats, negative comments or negative pictures or comments from other person. This is all done through core technologies described above mainly via online. Cyber Bulling can be done through chatting, instant messaging etc. Where website like Facebook, Orkut, Twitter user are more affected from Cyber Bullying. In my analysis generally feared person can reach a limit of depression, humiliation and threatens. Through this analysis we come to analyze that if person Bulled online he or she may be depressed up to the level of self harming. Having to use three attributes to describe internet fraud I would use the words intrusive, silent and dangerous. Just the silent mode of this type of crimes is a major problem in combating the threat, in fact, very often the companies realize that they have been victims of frauds or attacks until long after the event occurred. The consequences are disarming and retrieve the situation is sometimes impossible, precisely the time gap between the criminal event and its discovery provides an advantage to those who commit crimes often unbridgeable that makes impossible any action of persecution. But we are assuming

that the event is discovered by the victims and this is not always true, many companies are in fact over the years are victims of internet fraud, but they are not aware, a cancer that destroys from within.

According the report "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Companies" published by the Ponemon Institute, a study is based on a representative sample of 50 larger-sized organizations in various industry sectors, despite the high level of awareness of the cyber threat the impact of internet fraud has serious financial consequences for businesses and government institutions. The report shows that the median annualized cost of internet fraud for 50 organizations is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. The total cost is increased if compared to the first study of the previous year. The following chart demonstrate that virtually all companies experienced attacks moved using malware, very interesting also the data related to the action made by the insider and the damages caused by social engineering attacks. The conclusion is that industries fall victim to internet fraud, but to different degrees and with different economic impact. Defense, utilities and energy, and financial service companies experience higher costs than organizations in retail, hospitality and consumer products. The data provided give a clear situation regarding the impact of the internet fraud on the business of large size companies, however a significant impact is observed on the small business where the companies face the cyber threats with fewer resources and accepting the risks related to exposure. In this market segment internet fraud is very fierce and daily it tries to elude helpless companies that often fail to meet the cyber threat, the related damages are devastating causing in many situations the end of the business. In this sector is desirable for governments to support small businesses in harmony with a cyber-strategy defined at the national level. Leave helpless the social fabric made up of small businesses has definitely a direct impact also on the business of large firms.

The information revolution, coupled with the strategic leveraging of the Internet, has exposed a number of relatively open societies to the dangers of cybercriminal and cyber terrorist acts, especially in commercial business transactions. With the development of e-commerce, this commercial dark side has become known as internet fraud and has taken on many forms that affect the perceptions of the way we shop online. Corporations should realize that these threats to their online businesses have strategic implications to their business future and take proper measures to ensure that these threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained. These counter measures, coined as cyber security, have been developed

to ensure the safety of consumer privacy and information and allow for a carefree shopping experience. There is need for the development of models that will allow corporations to study the effects of internet fraud on online consumer confidence and to counter through leveraging the benefits associated with the latest developments in cyber security. With these two facets of e-commerce impacting the online consumer, corporations must ensure that the security measures taken will ultimately prevail to assure that consumers will continue to use the Internet to satisfy their shopping needs.

The first study to examine the emotional impact of internet fraud, it shows that victims' strongest reactions are feeling angry (58%), annoyed (51%) and cheated (40%), and in many cases, they blame themselves for being attacked. Only 3% don't think it will happen to them, and nearly 80% do not expect cybercriminals to be brought to justice— resulting in an ironic reluctance to take action and a sense of helplessness. "We accept internet fraud because of a 'learned helplessness'," said Joseph LaBrie, PhD, associate professor of psychology at Loyola Marymount University. "It's like getting ripped off at a garage – if you don't know enough about cars, you don't argue with the mechanic. People just accept a situation, even if it feels bad. "Despite the emotional burden, the universal threat, and incidents of internet fraud, people still aren't changing their behaviors - with only half (51%) of adults saying they would change their behavior if they became a victim Internet fraud victim Todd Vinson of Chicago explained, "I was emotionally and financially unprepared because I never thought I would be a victim of such a crime. I felt violated, as if someone had actually come inside my home to gather this information, and as if my entire family was exposed to this criminal act. Now I can't help but wonder if other information has been illegally acquired and just sitting in the wrong people's hands, waiting for an opportunity to be used." The "human impact" aspect of the report delves further into the little crimes or white lies consumers perpetrate against friends, family, loved ones and businesses. Nearly half of respondents think it's legal to download a single music track, album or movie without paying. Twenty-four percent believe it's legal or perfectly okay to secretly view someone else's e-mails or browser history. Some of these behaviors, such as downloading files, open people up to additional security threats. According to the FBI and the Department of Justice, cyber-crime is on the rise among American businesses, and it is costing them dearly. Cyber-crime includes a myriad of devious criminal practices designed to breach a company's computer security. The purpose of the electronic break and enter can be to steal the financial information of the business or its customers, to deny service to the company website or to install a virus that monitors a company's online activity in the future.

The-Cost-Of-Protection Companies that want to protect themselves from online thieves have to pull out their wallets to do it. There are costs in identifying risks, building new and safer operating procedures, and buying protective software and hardware. For businesses with complex or sensitive operations, this often involves hiring a cyber-security consultant to develop a customized solution. Not only are the upfront costs of protection expensive, but the systems must be tested and monitored regularly to ensure that they are still effective against emerging cyber-attacks. These costs are often passed on to the customer through higher prices of goods and services.

Lost-Sales Cyber-crime isn't just for thieves anymore. A new subculture has emerged in the past few years: the cyber-activist. These are the online equivalents of protesters who chain themselves to buildings or trees. Their purpose is to shut down a company's online operations to send a message about the company's business practices. In the past two years, major corporations, such as PayPal and MasterCard, have been attacked in this way. In December 2010, the PayPal website was attacked by dozens of people claiming to be part of the group, Anonymous. They attempted to perpetrate a denial of service attack in retaliation for PayPal shutting down payment services to Wiki Leaks. More than a dozen hackers were arrested in that crime.

While PayPal did not experience a full shutdown, many other businesses aren't so lucky. A denial of service attack results in fewer sales as customers cannot access the company's online store. It can even result in less revenue in the long-term if some customers decide to no longer do business with a company vulnerable to attack.

CONCLUSION AND RECOMMENDATIONS

The menace of internet fraud has eaten deep into the fabrics of our society and poses threats to the socio-economic development of the country. It is pertinent to state here that although internet fraud is a global phenomenon, the vulnerabilities and impact trends do tend to differ depending on the strength of the measures each country put in place to combat menace such as cyber laws and cyber protection technologies. Sadly, as shown in the arguments above, Nigeria ranks high amongst the internet fraud impacted countries however the country's response to mitigate internet fraud is still very low due to inadequate internet fraud legislations, limited technology and lack of cyber security experts. The shortage of human capital in cyber-security hence becomes a major vulnerability factor in addressing Nigeria's security needs to combat internet fraud and cyber threats emanating from cyber criminals. For example, Saulawa and Abubakar, (2014), posits that the Indian government is earmarking to develop five million cyber security experts in the next three years, while North Korea has already sponsored15,

000 cyber security experts with China having over 25 million cyber commandoes; with Nigeria needing nothing less than one million cyber security experts in the next two years to combat internet frauds. This should be supported by aggressive mass sensitization of the citizenry on the nature, schemes and tactics utilized by cybercriminals as a means of reducing their vulnerability. Following these submissions, the paper concludes that efforts by the government and the citizenry geared towards curbing internet frauds must be reinvigorated as cyber security is crucial for maintaining the continuity of vital social services, preservation of public trust in information systems and promotion of socio-economic development in Nigeria.

Following the conclusion reached in this study, the following recommendations have been proffered:

1. The government should pursue aggressive public sensitization against internet fraud using the mass media and the promotion of personal cyber space security should be incorporated in the primary, secondary and tertiary education curriculum.
2. Individuals need to observe simple personal safety rules such as not disclosing to strangers personal effects and banking details such as credit card pins, bank account numbers, e-mail codes and use of antivirus on their systems against malware etcetera.
3. Government and private sector should provide jobs for young graduates and where jobs are not readily available vocational skills and entrepreneurial development programmmes should be developed to reduce the number of youths getting involved in internet fraud.
4. In order to effectively curb the rate of internet fraud, the government needs to enact comprehensive laws to punish offenders.

REFERENCES

Abubakar, A.S. (2009). Investigating fraud schemes in Nigeria. *International conference on corporation against cybercrime, Strasbourg 10-11,* PP.1-5.

Adalemo, I. A. (1999). Youth and the city: An urban environment perspective. *Workshop proceedings on youth and the city: A study of Lagos Development Researchers' Corporative.*

Adebusuyi, I. & Adeniran, A. I. (2008). *The internet and emergence of yahoo boys sub-culture in Nigeria.* Ile- Ife. Nigeria. Obafemi Awolowo University press.

Ademola, C.O. (1999). *The future of ICT in Nigeria.* Lagos: Firm Publishers.

Adeniran, A. I. (2006). *A non- dependent framework for development.* Retrieved on 15th December 2021 from www.alder-consulting.com.

Adeniran, A.I. (2008). The internet and emergence of internet fraud in Nigeria. *International journal of cyber criminology 2(2) 368-381.*

Adeniyi, P.O. (1999). Youth and nation building: A continues challenge in Nigeria. *Workshop proceedings on youth and the city. A study of Lagos Development Researchers' Cooperative.*

Adeniyi, P.O. & Sackson, M. (1999). Computer ethics: Are students concerned. *First annual ethics conference.* Available online at: http://www.maths.luc.edu/ethics 96/papers/sackon doc.

Adler, F., Mueller, G.O.W & Laufer, W.S. (1995). *Criminology* (2nd Eds.). New York: McGraw Hill Inc.

Adomi, E.E. (2008). *Security and software for cyber cafes.* USA: IGI Global.

Adomi, E.E. & Igun, S.E. (2008). Combating internet fraud in Nigeria. *American journal of criminology*,19- 26(5).

Agboola, A.A. (2006). Electronic payment system and tele-banking services in Nigeria. *Journal of internet banking and commerce,* Vol.11, No.3.

Aghatise, E. J. (2006). Internet fraud definition. *Computer Crime Research Center, June 28, 2006.* Available online at: http/www.research.org.

Akinola, A. (2006). Cyber criminals on the loose. *Punch Newspaper*, Wednesday January 4.

Ani, L. (2011). Internet fraud and national security: The role of the penal and procedural law and Security in Nigeria. *African journal of e-crime, vol.1. 200-202.*

ANFIC, (2012). *American National Fraud Information Center.* Available at: http/www.anficinfo.com

Ayoku, A. O. (2005). The evolving sophistication of internet abuses in Africa. *The International Information and Library Review,* 37 (1) 11-17.

Basil, U. (2007). National cyber security strategies: Case study of Nigeria. *Africa Regional Conference on Cybersecurity, Yamousouko, Ta Technology.*

Charles, J.O. (2005). *Social anthropology. Concepts, theory & ethnography.* Lagos, Nigeria. Serenity Publishers.

Chawki, M. (2009). Nigeria tackles advanced fee fraud. *Journal of information Law and Technology, 1.*Available online at: http://en.wikipedia.org/wiki/Advance_ fee_ fraud.visited 28 October, 2021.

EFCC, (2004). *Economic and Financial Crime Commission Enactment Act, 2004.* Available online at http://www.efccnigeria.org.Visited 15th October, 2021

.EFCC, (2012). 288 jailed for internet fraud. *Economic and Financial Crime Commission News.* Retrieved on 15th July 2021 from http://www.efccnigeria.org/20120402_court_jails.html.

ICCC (2010). *Internet crimes complaint center reports.* Available online at http://www.ic3.gov/faq/default.asp. Accessed march 18,2021.

Idom, A. M. (2012). *Fiber optics technology and internet frauds in Cross River State: A proactive analysis.* Unpublished seminar paper presented in the Department of Sociology, University of Calabar.

Ige, O. A. (2008). *Secondary School Students' perceptions of incidence of internet crimes among school age children in Oyo and Ondo States, Nigeria.* Unpublished Masters Dissertation in the Department of Teacher Education, University of Ibadan.

Igbo, E. M. (2008). *Aetiology of crime: perspectives in theoretical criminology.* Enugu. New Generation Books.

Iwarimie – Jaja, D. (2012). *Criminology, the Study of Crime, 4th Edition.* Owerri: Springfield Publishers Ltd.

Katyal, K.N. (2003). Digital architecture as crime control. *The Yale law Journal,* 112 (8) 2261-2289.

Longe, O.B. & Chiemeke, S. C. (2007). Information and communication technology penetration in Nigeria: prospects, challenges and metrics. *Asian Journal of Information Technology,* 6 (3).

Longe, O.B. & Chiemeke, S.C. (2008). Internet fraud and criminality in Nigeria- what roles are internet access points playing. *European Journal of Social Sciences,* Vol. 6, No. 4.

Mabogunje, A. L. (1999). Challenges of a u- turn generation: Youth and national sustainable development. *National Conference on Youth Development in Nigeria. Abuja.*

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review.* 3:672–682. DOI: 10.2307/2084686

Microsoft Company (2011). *Piracy of microsoft word operation windows.* Microsoft Nigeria.

Ninalowo, A. (2004). *Essays on the state and civil society.* Lagos: First Academic Publishers.

NFIC, (2007). *National Fraud Information Center.* Available at: http/www.nficinfo.com

NPF (2012). Nigerian Police Force; Cross River State Crime Investigation Department.

NPFIT (2001). *National Policy for Information Technology.* Federal Republic of Nigeria.

Ogwezzy, M. C. (2012). Cybercrime and the proliferation of yahoo addicts in Nigeria. *International Journal of Juridical Sciences, No. 1 PP 86-102.* Available online at htpp://www.jurdicaljournal.univagora.ro. Visited 12th March, 2021.

Okeshola, F.B. & Adeta, A.K (2013). The nature, causes and consequences of internet fraud in tertiary institutions in Zaria-Kaduna State, Nigeria; *American International Journal of Contemporary Research*, Vol.3 No 9.pp. 19-114.

Olaide, J. & Adewole, O. (2004). Cybercrime embarrassing for victims. *American Journal of Criminology, Vol.1* No.2.Retrieved September, 2021 from http//www.heraldsun.com.au

Onwunyi, U.M & Okonkwo, K. J (2021), Youths and Internet fraud In Nigeria: Implications of the Nationwide Covid 19 Lockdown, *International Journal of Legal Studies and Research, 2 (3)*

Oludayo, T. & Ibrahim, A. (2011). Social organization of internet fraud among University Undergraduates in Nigeria. *International Journal of Internet fraud,* Vol. 5 (2): 860-875.

Phonesolution, (2005). *Basic software phone repairs and viruses in Calabar.* Calabar, Nigeria. Serenity publishers.