Covenant Journal of Business & Social Sciences (CJBSS) Vol. 12 No.1, June, 2021

ISSN: ***p. 2006-0300 e. 2334-5708*** **DOI:**

An Open Access Journal Available Online

INTERNET FRAUD AND ITS EFFECT ON NIGERIA'S IMAGE IN INTERNATIONAL RELATIONS

Eze-Michael, Ezedikachi. N (PhD)
Lecturer of International Relations / International Law
Department of Political Science, Public Administration
Babcock University
eze-michaele@babcock.edu.ng
Phone No: +2348061321140

Received: 15.1.2021 Accepted: 15.2.2021

Date of Publication: June, 2021

INTERNET FRAUD AND ITS EFFECT ON NIGERIA'S IMAGE IN INTERNATIONAL RELATIONS

ABSTRACT: Internet fraud has become an increasing form of computer crime. This study investigated the effects of internet fraud on Nigeria's image in international relations. The study adopted quantitative method and descriptive survey. Journals and materials from internet complemented the major sources. Findings showed that unemployment and poverty are major causal factors of internet fraud. The study concluded that, internet use by Nigerians has come with fraudulent acts, and this has put Nigeria under scrutiny and brought negative image in international relations. The study recommended that, government should enact a comprehensive law on internet fraud and empower graduates by providing employment.

Keywords: Fraud, Internet, Internet fraud, Image, Nigeria's image, International relations

1. INTRODUCTION

The contemporary world of the 21st century has come a long way from the era of no internet, with most people unable to recall how majority of activities were accomplished in the past without the use of internet. For example, current undergraduate students' commendation is always given to those whose era of educational experience was without the use or provision of the internet for purposes such as term papers, assignments, research and even communication. In essence, the development of the Internet is regarded as a paramount innovation as it has fostered different developments in the world including globalization. This has benefited the world over, including Africa.

In 1996, seven years after the internet was first introduced in the United States of America, it was also introduced in Nigeria and with it came amenities, job opportunities and the emergence of network providers. It is general knowledge that every development has its beneficial and adverse effect; the latter for Nigeria is the rampant use of the internet as a medium for fraudulent activities termed "Internet fraud" which is criminal activities majorly for the purpose of exploiting individuals. It is a multi-dimensional and intrinsically complicated problem. It has taken different forms containing numerous facets such as Online intellectual property theft,

Identity theft, phishing, Page jacking, Advance fee scams, Bad check scams, Fake money orders, Wire transfer fraud, anonymous servers, hijacked emails, fake websites being used as tools and medium for fraud by perpetrators. In the last decade, the image of Nigeria and Nigerians took a very hard hit as internet scams and fraud assumed increasingly alarming and frightening dimensions. As internet scams and fraud got on the rise, the image of Nigeria seems to be synonymous with these scams. In 1989 and 1990 before the internet age, Nigerians were involved in cross border defrauding with the use of telex and written letter which is why with the advent of the internet Nigerians were wrongfully viewed as the progenitors of most internet scams because of how notorious citizens of the country became in the act all over the world. The Federal Bureau of Investigation took an interest in the investigation of internet fraud and as stated on their website (www.fbi.gov) the "Nigerian letter or 419 fraud" is of major target due to its notoriety. The name '419'comes from the section of the Nigerian Criminal Code dealing with fraud. In some cases this type of fraud is referred to as advance-fee fraud.

The table above elucidates the rate at which Nigerians have been engaging in internet fraud since the late 1990s and early 2000s a few years after internet was introduced into Nigeria.

By year 2006, there was a significant escalation in the rate of internet fraud among Nigerians. In

Year	**Data**
2001 and 2002 (FBI)	15.5 % of Internet Fraud report were Nigerian 419 scams, Median Loss for 419 was highest at $5,575
2002 ANFIC	Nigerian Money Offers, 4% of total Internet fraud worldwide. (American National Fraud Information Center)
2003 (VeriSign)	Nigeria is 3rd in the world in the total Number of fraudulent, internet transactions, with 4.81% of world Internet fraud
2004 (Reuters)	48% of global email is Spam, 6% is Nigerian Email

2010, the Internet Crime Complaint Centre ICC, which is a partnership between the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre, revealed that Nigeria was ranked third among the list of top ten sources of cybercrime in the world with 8% behind the US (65%) and the UK (9.9%) (Daily Trust, 2010).

The Image a country portrays in the international system and in relations to foreign states plays a big role in determining its standpoint, recognition and credibility in the international system. The issue of internet fraud is not favorable to a country's image and reputation. It portrays a level of involvement in criminal activities which scares away investors, discouraging local and foreign investment which is not good for the economy. It causes erosion in international and public confidence concerning the country's financial sector. It discourages hard work in academic settings which is understandable especially; as it is assumed that most perpetrators of internet fraud are students of tertiary institutions.

Nigeria as a country currently has some laws that regulate the activities of the cyberspace. Such as the Economic and Financial Crime Commission (EFCC) Act, Money laundering Act and the Advance Fee fraud Act. A ricochet of an adverse effect caused by internet fraud is that Nigerian ISPs and email providers are being black-listed in e-mail blocking systems across the Internet. The implication of this is that some countries websites like eBay do not receive materials from Nigerian ISPs. All the above can be very detrimental to Nigeria's image in the international system causing numerous strain on its political, economic and diplomatic relations with other states. This, therefore, has necessitated Nigeria to take a stance in combating the issue of internet fraud and reform its image in the international system. It is against this backdrop that the study examines internet fraud and how it affects Nigeria's image in the international relations

2. CONCEPTUAL PERSPECTIVE ON THE USE OF INTERNET

According to Vladimir (2005) internet is a global network which is meant to unite millions of computers located in different countries and opens broad opportunities to obtain and exchange information but it is now being used for criminal purposes due to and especially, the economic factors. Nigeria is faced with economic challenges such as poverty, unemployment, corruption, amongst others, thereby making this crime thrives.

Prior to the advent of internet, there have been habitual commissions of fraud. Fraudsters carried out their operations in different ways and forms across the globe. Those who attempt fraud on the internet are just the latest in a long line of those trying to con the unassuming. In the early 80s and toward late 90s, there witnessed the production and distribution of counterfeit money. With one of the most imperative discoveries of the twentieth century, the internet fraud is much easier now for criminals as they are capable of acting beyond national boundaries and their

immediate environment. Recently, the mode of contacting victims has been widened since the fraudsters need not to be physically present to commit the fraud. Longe and Chiemeke (2006) posited that fraudsters pick victims and approach by letter, faxes or electronic mail, without prior contact. Victims' contacts and addresses are obtained from telephone and email directories, business journals, magazines, newspapers or through web e-mail address harvesters. What can be said is that fraudsters generally have taken advantage of the advent of internet to advance and change their modus operandi. Now those engaged in this type of fraud, can seat in the comfort of their homes or cyber cafes and reach out to unsuspecting victims from different parts of the world. In this section, the study will be examining the historical background of internet fraud in Nigeria, meaning of internet fraud, theory of crime and fraud and the different types of internet fraud.

2.1 *Internet fraud in Nigeria*

The history and growth of internet in Nigeria can be traced to 1995, when The Nigerian Internet Group was formed; this is a non-governmental organization, with the objective of facilitating the full access to internet in Nigeria. This group was formed after the first internet workshop organized by the Yaba College of Technology in collaboration with a number of organizations including the Nigerian Communications Commission, National Data Bank, Literacy Training and Development Program for Africa (University of Ibadan) and Administrative Staff College of Nigeria (ASCON), with direct assistance from the United States Information Service (USIS), Regional Information Network for Africa (RINAF) and the British Council. In 1996, seven years after the introduction of internet service in United States, the Nigerian Communications Commission decided to license 38 internet service providers to sell internet services in Nigeria. The very first internet service provider "Link serve Limited" began operation in 1st of January 1997. (Vanguard Nigeria, 2010).

Another major African seminar was held in May 1999, where internet policies were made for African countries. It was organized by the Ministry of Communication and titled Africa Internet Summit (AFRINET 99). The research on the growth of internet usage in Nigeria was carried out by the International Communication Union between the periods of 1996 -2009. They reported as follows; in 2000, it was 0.3% it moved up a little between 2002 and 2004, when it rose to 1.5%, by 2007 it had escalated to 7% and by 2008, it rose speedily to 15%. The research showed that as

at 2007 Nigerians were the highest users of internet, but by 2009 Egyptians took over with 17% users in every 100 people, compared to Nigerian users of 15% in every 100 people. Currently in Nigeria, internet is available in every urban area, it is much easier as one can access it even on a mobile telephone. Often times, readers tend to misunderstand the meaning of internet fraud, and sometimes substitute the term cybercrime for internet fraud. However, what must be noted is that internet fraud is one of the types of cybercrime. Other types of cybercrime include, cyber stalking, cyber bullying, online trafficking, child pornography, cyber terrorism and many more. Computer fraud is the only term that is used interchangeably with internet fraud while cybercrime is an umbrella for all forms of cyberspace perpetrated illegality.

The historical development of internet fraud in Nigeria is contentious. There have been diverse opinions on the actual regime and era that the fraud began in Nigeria. Though not a new concept, it is believed that it went rampant during the Shagari administration due to programs and policies introduced by the government during the period of his reign. History has shown that fraud began excessively during the Shehu Shagari regime, while some others believe that it was during the military era, these diverse views will be synchronized and synergized to produce a singular and comprehensive historical background to internet fraud in Nigeria. The term "419" is coined from section 419 of the Nigerian criminal code. Section "419" of the criminal code, laws of the federation of Nigeria and Lagos (1958) Chapter 42, states unequivocally that;

"Any person who by any false pretense and with intent to defraud obtains from any other person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. If the object is valued for five hundred pounds or upwards, he is liable to imprisonment for seven years. It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretense…"

Though this section has been engraved in the Nigerian criminal code since 1958, it was just a section like any of the five hundred and twenty one sections in the code and did not beg for particular attention or distinction from other offences in the code. Modern scams have been linked and associated with Spanish prisoner scam dating of 19th century. The system of operation was that businessmen will be contacted by an individual allegedly trying to smuggle someone connected to a wealthy family out of prison in Spain. They will inform their targets to part with some amount of money to bribe the prison officers and promised to share the proceeds of the

work with the targets after the operation. (Brunton, 2013), On the history of 419 scams in Nigeria traced the history of the scams to ''Second Republic between 1979 to 1983'' under the administration of then President Shehu Shagari. According to the source, the modus operandi was such that many variants of the letters were sent. The example of such letter sent via postal email was addressed to a woman's husband and inquired about his health and a long, unexpected silence. It then asked what to do with profits from a $24.6 million investment, and ended with a telephone number. Other official letters were sent from a writer who said that he was a director of the state owned Nigerian National Petroleum Corporation. He said that he wanted to transfer $20 million to the recipient's bank account money that was budgeted but was never spent. In exchange for transferring the funds out of Nigeria, the recipient would get to keep 30% of the total amount. To start the process, the scammer asked for a few sheets of the company's letterhead, bank account numbers, and other personal information.

The above established that fraud and fraudsters have been in existence since time immemorial, and since the twenty first century era of the emergence of internet and computers, it is expected that fraudsters also change their modus operandi to be in sync with modern technologies and approaches.

EFCC (2006) reported the rate of internet crime in Nigeria and the position of the country amongst other countries where cybercrime is prevalent. The publication reported a retired civil servant with two other accomplices who defrauded a German citizen, Klaus Wagner a sum of USD 1, 714,080 through the internet. Ribadu (2007) the pioneer Chairman of EFFC posited that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase and other e-commerce kind of fraud. His position was later corroborated by the statement of Olugbodi (2010) where he opined that the most prevalent forms of cybercrime are website cloning, financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, fraudulent electronic mails, cyber laundering and virus/ worms/ Trojans. The study shall consider the following examples of the most frequent types of Internet fraud

1. **Romance scam**

   Great Britain has the highest victims of romance scam. The research in 2012 showed that more than 230,000 people may have fallen victims of romance fraudsters in Great Britain alone (Whitty & Buchanan, 2012). One can opine that romance scammer works on the

mentality and emotion of their victims, what they tend to achieve is to lower the defences of their victims by appealing to their romantic or compassionate side. They play on emotional triggers to get their victims to provide money, gifts and personal details.

At the early stage of the relationship, giving of minor gifts may be reciprocal. Then eventually the scammer makes requests for small amounts of money for numerous reasons.

2. **Lottery scam**

As the name implies, there are so many sites, that offer fake lottery and in most cases victims supply sensitive information to these sites. It operates in this manner; an email is received from a lottery institution congratulating the individual of winning a lottery they did not participate in. The scammers usually demands for quick response from their victims. In addition they advise victims to keep their winnings private to maintain security of the price won. The real scam comes when the victims are asked to pay some amount of money or fees to release their winning prize. Scammers often refer to these fees as insurance costs, government taxes, bank fees, etc.

3. **Phishing**

Phishing is a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers (See Anti-Phishing Working Group, 2004). The origin of the word is traced to the analogy that scammers are using email lures to fish for passwords and financial data from the sea of Internet users. Another name for phishing is brand spoofing; it is the creation of email messages and Web pages that are replicas of existing and legitimate sites. These Web sites and emails are used to trick users / victims into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud. The sole aim of the phishing scammers is to establish in the subconscious of the victims that, information they received is from a genuine websites and thereby established their faith in them.

4. **Cheque overpayment scam**

This is particular to those that engage in buying and selling on the internet, especially those that are selling something on the internet, they may be approached or targeted by cheque overpayment. The operation is such way that, the seller might receive an offer from a buyer who is a scammer. After the offer, they intentionally write an overpayment cheque for the seller. Seller out of sincerity will alert the buyer, of the overpayment and the potential buyer scammer, will apologize thereby ask for the refund of the money through an online banking or through Western Union. The actual scam takes place, when the seller fail to cash the cheque before he/she sent the goods and the so called overpayment cash before he or she detects that the cheque will bounce or cheque bounces.

All these above mentioned methods or modes are the ways victims are deceived and fall prey to scammers. In the cases where prospected victims do not give in to the luring tactic of the scammer certain software's are used to penetrate the computers of unassuming individuals retrieving vital personal information which can be used to facilitate fraudulent activities. Examples of that software are malware, spyware and worm.

2.2 *Effects of internet fraud on Nigeria's image*

1. Tarnishing the country's reputation

Without any doubt, internet fraud has tarnished the image of this country in the international arena to an irreparable level. Cybercrime has created a bad image for Nigeria which has earned her a spot in the present ranking in Transparency International where Nigeria is being listed as one of the most corrupt nations in the world. (Folashade B. et. al 2013) and Adomi (2008) have concluded it, when he opined that cybercrime has created an image nightmare for Nigeria. He said that most scam e-mails are thought to originate from Nigeria or Nigerians which is actually not the case. Nigerians are treated with suspicion in business dealings and transactions.

2. Lack of trust and confidence hinders profitable transaction

Nigerians are not trusted when it comes to business transaction in most countries abroad, the major reason for this is the level of fraudulent activities committed in their country that have been attributed to Nigerian citizens, therefore foreigners find it difficult to trust Nigerians because of fear of losing their money and goods. In many cases online transactions would be made but the buyers never receive goods from sellers, this is why some online shopping sites

refuse to include Nigeria on their list of countries for delivery e.g. eBay. According to reports sponsored by the Better Business Bureau online over 80% of online shoppers cites security as their primary concern when shopping online. About 75% of shoppers terminate the transaction when asked for their bank card details. The level of decadence of the Nigerian reputation has caused her citizens to be treated with suspicion in most or all their business dealings (Adomi, 2008).

3. Denied opportunities for Nigerians abroad

The situation of Nigeria's image is in direct comparison with the famous saying "One bad apple would spoil the bunch" because majority of Nigerians who do not have the slightest idea of what it takes to be a fraudster are suffering under the bad reputation umbrella created by those Nigerians caught. Nigerians are hardly considered when they seek asylum in foreign countries especially in the United Kingdom because of this bad reputation. In the last fifteen years only one out of ten of the 13000 asylum claims have been accepted. (Freeman, 2016). Folashade B. et. al 2013, opined that cybercrime has negative consequences. Cybercrime threatens foreign investment as well as misrepresents the country among other nations as corrupt. It will also lead to stigmatization of business men and women and they will face certain barriers when carrying out legitimate businesses. Majority of the business men and women go through a strenuous screening before foreigners would eventually agree to transact business with them.

4. Inimical to the progress and development in the country

Foreign direct investment is one of the major forms of economic development for a country and the refusal of foreign companies to invest may cause a retarded growth however significant in the economy of the home country. Fear of fraud is a major deterrence for foreign companies. The inevitable cycle of events if this continues, would result into "No Investment No Development, No Development No Employment and No Development and Employment No Progress". The amount of business deals and investment prospects that have been lost by Nigeria as a country due to fraudulent speculations is enough to make a significant change in all federating states of Nigeria (Folashade, 2013).

2.2.1 Differential association theory of crime: Edwin Sutherland, an American sociologist, propounded this theory. The central point of this theory is that, through interaction with others, individuals learn the values, attitudes, techniques and motives for criminal behavior. To those

that belong to this school of thought, it is believed that the environment plays a vital role in formulating the behavior of an individual. To Sutherland, he believed that the environment plays a major role in deciding which norms people learn to violate (Sutherland, 1939).

The principle of differential association asserts that a person becomes delinquent because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of law. What this means is that an individual will become a criminal because they are exposed to more favorable criminal behavior. What this explains for instance, is that where we have five people, four of them are criminals, the fifth person may on the long run be influenced by the activities and action of these other four and then learn the act of criminality of these people, and may eventually join them. The basic point of Sutherland is that criminal behavior is learned (Sutherland 1939). Communication is the major tool of learning criminal behavior; it is learnt through interactions with the perpetrators of crimes and by befriending them. The principal part of the learning of criminal behavior occurs within intimate personal groups. The best way to learn criminal behavior is by learning the technique for committing the crime. It means that to know how to perpetrate internet fraud, what is needed to be done is to learn the technique from veteran perpetrators. This explains the ever increase in the number of yahoo boys in our various university campuses.

From the above background on differential association theory, it is clear that the theory can be applied to cybercrimes. The focal point of this theory is that criminal behavior is learned through social interaction with others. The medium of social interaction for most internet fraudsters may come through electronic communications with other individuals who share similar interests.

3. DATA PRESENTATION, ANALYSIS AND INTERPRETATION

Table 1: Internet sites used mostly by the respondents

	Frequency (N)	**Percentage (%)**
Facebook	176	44.0
Yahoomail	44	11.0
Yahoo Messenger	104	26.0

Skype	56	14.0
Others	20	5.0
Total	400	100.0

Source: *Field survey, 2016*

Table 1 above shows the types of social media that are in use. The table reveals that 44.0% of the respondents are Facebook users, 11.0% of the respondents are users of yahoo mail, 26.0% of the respondents are yahoo messenger users, 14.0% of the respondents use Skype and 5.0% of the respondents use other internet sites. This shows that majority of the respondents are Facebook users.

Table 2: Frequency of using the internet and other networking sites

	Frequency (N)	**Percentage (%)**
Always online	176	44.0
Daily	104	26.0
Twice daily	56	14.0
Occasionally	44	11.0
Total	100	100.0

Source: *Field survey, 2016*

The table 2 above explains the rate of internet usage by Nigerian citizens. The table explains that 44.0% of the respondents are always online, 26.0% of the respondents use the internet daily, 14.0% of the respondents use the internet sites twice daily while 11.0% of the respondents use it occasionally. However, this table shows that majority of internet users are always online.

Table 3: Roles internet plays in the lives of average Nigerians

	Frequency (N)	**Percentage (%)**
Positive role	140	35.0
Negative role	180	45.0
Both	80	20.0

Total	400	100.0

Source: *Field survey, 2016*

Table 3 above explains the role of internet plays in the lives of average Nigerians. From the table, 35.0% of the respondents were of the opinion that internet plays a positive role in the lives of its users, 45.0% of the respondents were of the opinion that it plays a negative role in the lives of its users while 20.0% of the respondents believed that internet plays both a positive role and negative role in the lives of its users. Therefore, it can be deduced that internet plays more of negative role in the lives of its users as shown in the table.

Table 4: Means through which people use the internet

	Frequency (N)	**Percentage (%)**
Phone	180	45.0
Personal Laptop	120	15.0
Public Café	60	30.0
Others	40	10.0
Total	400	100.0

Source: *Field survey, 2016*

Table 4 above explains the means through which people use the internet. This table shows that 45.0% of the respondents access the internet by phone, 30.0% of the respondents access the internet by personal laptop, 15.0% of the respondent's access the internet by public café while 10.0% of the respondents access the internet by others means. However, majority of the respondents access social media by means of their phone.

Table 5: Respondents' level of exposure to internet uses

	Frequency (N)	**Percentage (%)**
High	260	65.0
Average	100	25.0
Low	40	10.0

Total	400	100.0

Source: *Field survey, 2016*

Table 5 above explains the respondents' level of exposure to the internet. This table shows that 65.0% of the respondent's level of exposure to the internet is high, 25.0% of the respondents have a moderate exposure level to the internet and 10.0% of the respondents have low level exposure to the internet. This shows that majority of the respondents level of exposure to social media is high.

Table 6: Showing the major causes of internet fraud

	Strongly Agree		Agree		Disagree		Strongly Disagree	
	N	%	N	%	N	%	N	%
Unemployment	196	49.0	80	20.0	32	8.0	92	23.0
Poverty	120	30.0	112	28.0	120	30.0	48	12.0
Peer group influence	148	37.0	128	32.0	76	19.0	48	12.0
Defective socialization	56	14.0	176	44.0	68	17.0	100	25.0
Weak laws	92	23.0	144	36.0	88	22.0	76	19.0
High level of corruption	192	48.0	104	26.0	48	12.0	56	14.0
Easy accessibility to internet	100	25.0	64	16.0	136	34.0	100	25.0

Source: *Field survey, 2016*

Table 6 showed that virtually all respondents (69.0%) agreed that unemployment is a causal factor of internet fraud as against 31.0% who disagreed on unemployment as one of the major causes of internet fraud. Also, 58.0% were of the view that poverty is a major cause while 42.0% of the respondents disagreed. 86% of the respondents opined that peer group is the cause of internet fraud.

3.3 The types of internet fraud mostly found among Nigerian citizens

Table 7: Showing the types of internet fraud among Nigerian citizens

	Strongly Agree		Agree		Disagree		Strongly Disagree	
	N	%	N	%	N	%	N	%

Hacking	140	35.0	176	44.0	60	15.0	24	6.0
Credit card fraud	88	22.0	188	47.0	84	21.0	40	10.0
Software piracy	116	29.0	192	48.0	56	14.0	36	9.0
Cyber identity theft	148	37.0	136	34.0	80	20.0	144	9.0
Cloning of website/Phishing	128	32.0	180	45.0	90	18.0	20	5.0
Pornography	184	46.0	140	35.0	48	12.0	28	7.0
Sweet heart swindle (Social network)	88	22.0	188	47.0	84	21.0	40	10.0
Cyber defamation	200	50.0	80	20.0	100	10.0	80	20.0
Malicious program/Virus dissemination	116	29.0	192	48.0	56	14.0	36	9.0

Source: *Field survey, 2016*

Table 7 above shows the common types of internet fraud in Nigeria. Findings reveal that majority of the respondents are of the view that hacking (79.0%) and credit card frauds (69.0%) are the common type of internet fraud in Nigeria. However, malicious program and virus dissemination (32%) and cyber stalking (27%) which are other types of internet fraud got low response from the respondents. Other types of internet fraud aside the listed ones that are common in Nigeria according to respondents includes alteration or disclosure of data, trafficking in passwords and credit card number, lottery, educational scam where students only pay half the tuition fees and stealing of direct TV signals by modifying the card that goes into the satellite receivers.

3.4 *Decadence of internet fraud on Nigeria's image*

This section delved into the consequences of internet fraud on Nigeria's image in the international relations. This includes loss of life, tarnishing the country's image internationally, loss of revenue etc. Respondents were asked about the consequences of internet fraud.

Table 8:

	Strongly Agree		Agree		Disagree		Strongly Disagree	
	N	%	N	%	N	%	N	%
Tarnishing the country reputation	188	47.0	116	29.0	44	11.0	52	13.0
Lack of trust and confidence hinders	232	58.0	148	37.0	8	2.0	12	3.0

profitable Transaction								
Denial of innocent Nigerians opportunity abroad	120	30.0	140	35.0	92	23.0	48	12.0
Inimical to the progress and development in the country	200	50.0	64	16.0	96	24.0	40	10.0
Loss of employment	124	31.0	172	43.0	72	18.0	32	8.0
Loss of life	108	27.0	112	28.0	92	23.0	88	22.0
Loss of revenue	152	38.0	128	32.0	104	26.0	16	4.0

Source: *Field survey, 2016*

Table 8 above shows the negative consequences of internet fraud to the society. It was found that 76% of the respondents are of the view that internet fraud will tarnish the country's reputation internationally. Lack of trust and confidence which is currently hindering profitable transaction was also examined as 95% of the respondents agreed to this as against the minority (5.0%) who opined that internet fraud would not hinder profitable transaction as a result of lack of trust and confidence among Nigerians and their involvement in the international relations.

4. DISCUSSION OF FINDINGS

Internet fraudsters in Nigeria have recognized online opportunities to perpetrate online frauds. The National Fraud Information Centre (NFIC), in 2007 listed top ten reported Internet scams to include: fake Cheque scams (29%), general merchandise (23%), auctions (13%), Nigerian money offers (11%), lotteries (7%), advance fee loans (3%), prizes/sweepstakes (3%), phishing (3%), friendship and sweetheart swindles (1%) and Internet access services scam (1%)5. Of these, $4, 043.14 is lost by victims of the Nigerian money transfer scam. This is in tandem with Katyal (2002) posits that, at present, the damage caused by computer fraud runs to billions of dollars each year, making it one of the most economically damaging forms of crime in human history. Each day, more than half a billion people around the world log on to the Internet to buy and sell goods, to exchange ideas and to communicate promising opportunities and innovative solutions. As billions of dollars cut across the Internet each day, a small group of predators have chosen to make cyberspace a place for crime and fraud. Ige (2008) examined secondary school students' perceptions of incidences of internet crimes among school-age children in Oyo and Ondo States,

Nigeria. The study found that students are being initiated into internet crime by their friends in the universities, polytechnics, and colleges of education.

Furthermore, male students are more involved than their female counterparts, a reflection of what happens worldwide. Again the study discovered that, senior secondary school students' involvement in internet crime is not a function of the socioeconomic status of their parents, as students from both rich and poor homes engage in the crime. In addition to this, the involvement of students in internet crime has no effect on their academic performance, as the students' higher level of cognitive thinking being used to scam people on the internet is being exploited to enhance their academic standard. Adeniran (2008) contends that in Nigeria, unlike the traditional criminal groups, both sexes are functionally involved in internet fraud in Nigeria, with varying specialized functions. Reddick and King (2000) and Adeniran (2006) claim that the anonymity and privacy that the internet provides for potential users has excessively enhanced the degree of fluidity and structural complexity of the fraudsters operations in Nigeria. Today, they get access to the internet without leaving their homes. Embezzlements, electronic frauds, fictitious sales of properties and cars are all being carried out without leaving a trace.

Also, gender switching - a new sense of self that is "decentered and multiple" - has emerged among these fraudsters in Nigeria. This is essentially for the purpose of facilitating their nefarious activities. At a single point in time, an individual could claim to be a "beautiful lady" or a "big man" or a "celebrity", all depending on their immediate needs. Arowosaiye (2008) avers that fraudsters in Nigeria and their foreign counterparts are perfect exploiter of global financial growth and ICT advancement which renders traditional geographical expression meaningless. Today, it is possible to plan a crime in one country, carry it out in another and move the proceeds from one country to another or more countries, all from a personal computer.

The categories of economic and financial crimes in Nigeria are too wide to be exhausted here. However, the recent phenomenon of phishing, identity theft, credit card fraud, which are closely related forms of cyber or internet frauds and internet piracy are emerging economic crimes which need to be addressed by the existing Nigerian criminal law. Michael (2006) asserts that phishing, credit card fraud and identity fraud are not really distinct form of ICT enabled or internet economic crimes but rather another method of online fraud scheme. Using this method, fraudsters create websites that appear legitimate but in reality are scam designed to defraud or obtain information that can be used to commit further economic crimes.

Evidently, (13%), Nigerian money offers (11%), lotteries (7%), advance fee loans (3%), prizes/sweepstakes (3%), phishing (3%), friendship and sweetheart swindles (1%) and Internet access services scam (1%). Of these, $4, 043.14 is lost by victims of the Nigerian money transfer scam. Katyal (2002) posits that, the damage caused by computer fraud runs to billions of dollars each year, making it one of the most economically damaging forms of crime in human history. Each day, more than half a billion people around the world log on to the Internet to buy and sell goods, to exchange ideas and to communicate promising opportunities and innovative solutions. As billions of dollars cross across the Internet each day, a small group of predators have chosen to make cyberspace a place for crime and fraud. Ige (2008) examined secondary school students' perceptions of incidences of Internet crimes among school-age children in Oyo and Ondo States, Nigeria. The study indicated that students are being initiated into internet crime by their friends in the universities, polytechnics, and colleges of education. Furthermore, male students are more involved than their female counterparts, a reflection of what happens almost everywhere.

This study found that, senior secondary school students' involvement in internet crime is not a function of the socioeconomic status of their parents. This is because students from both rich and poor homes engage in this crime. In addition, the involvement of students in internet crime has no effect on their academic performance, as the students' higher level of cognitive thinking being used to scam people on the internet is being exploited to enhance their academic standard. Adeniran (2008) contends that in Nigeria, unlike the traditional criminal groups, both sexes are functionally involved in internet fraud in Nigeria, with varying specialized functions. Reddick and King (2000) and Adeniran (2006) claim that the anonymity and privacy that the Internet provides for potential users has excessively enhanced the degree of fluidity and structural complexity of especially the '*yahoo-boys*' operations in Nigeria. Today, they get access to the internet without leaving their homes. Embezzlements, electronic frauds, fictitious sales of properties and cars are all being carried out without leaving a trace. Also, gender switching - a new sense of self that is "decentered and multiple" - has emerged among the *yahoo-boys* in Nigeria. This is essentially for the purpose of facilitating their nefarious activities.

At a single point in time, an individual could claim to be a "beautiful lady" or a "big man" or a "celebrity", all depending on his/her immediate needs. Arowosaiye (2008) avers that fraudsters in Nigeria and their foreign counterparts are perfect exploiter of global financial growth and ICT advancement which renders traditional geographical expression meaningless. Today, it is

possible to plan a crime in one country, carry it out in another and move the proceeds from one country to another or more countries, all from a personal computer. The categories of economic and financial crimes in Nigeria are too wide to be exhausted here. However, the recent phenomenon of phishing, identity theft, credit card fraud, which are closely related forms of cyber, internet frauds and internet piracy are emerging economic crimes which need to be urgently addressed by the existing Nigerian criminal law. Michael (2006) asserts that phishing, credit card fraud and identity fraud are not really distinct form of ICT enabled or internet economic crimes but rather another method of online fraud scheme. Using this method, fraudsters create websites that appear legitimate but in reality are scam designed to defraud and obtain information that can be used to commit further economic crimes.

5. CONCLUSION

The remarkable development in human history through computer technology has no doubt brought transformation in all aspects of life, especially in communication and information technology. However, the embracement of the internet by Nigerians has come with a lot of fraudulent acts. Individuals, groups, companies and government establishments have been found to be defrauded through the internet. Nigerian people are valued in terms of what they possess and command economically. Conversely, those without economic success are undervalued and the pressure to achieve success is intensified. This necessitated some Nigerian individuals to devise survival strategies to attain economic success, thereby causing them to indulge in cybercrime. However, this has put Nigeria under negative scrutiny and that is not good for our image in international relations. Based on the findings and conclusion of this study, the following recommendations are made:

1. Education is the most vital weapon for literacy; as such seminars and workshops should be organized from time to time with emphasis on internet safety. This will make the individuals learn to keep their personal information safe and youth will flee cybercrime.
2. The study shows that youths involved in internet fraud are either in tertiary institutions or have graduated from tertiary institution. It is therefore, recommended that curriculum which will include courses on internet fraud, internet management and its prevention should be introduced to both tertiary and secondary schools to take care of the present social changes.

3. For government agencies, law enforcement agencies, intelligence agencies and security agencies to fight and curb internet fraud, there is need for them to understand both the technology and the individuals who engaged in this criminal act.
4. Cyber criminals' assets should be confiscated by the government if discovered. There should be imposition of 25 year-jail term for cyber-crimes. This will serve as deterrence to those youths who may want to indulge in such crime.
5. Internet users should inculcate the habit of continuously updating their knowledge about the ever changing nature of ICTs, through this, they will not only be well informed about the current trends in cybercrimes, but also be security conscious.

Suggestion for Further Studies

1. A study can be carried out to determine the effect of internet fraud on Nigeria populace using a wider scope of study.
2. A study can be carried out concentrating on students alone and their use of internet sites to determine the level of decadence this may cause on the Nigeria system and on the international system.
3. A study can also be carried out to examine cybercrime rates and other fraudulent act on the part of Nigerian youth and its effect on the global world and in international relations.

Refrences

Abiola, J. (2013). The Impact of Information and Communication Technology on Internal Control's Prevention and Detection of Fraud.

Adebayo, H. (2015, october 8). Premium times. Retrieved from http://www.premiumtimesng.com/news/top-news/191241-u-s-indicts-9-nigerians-over-online-romance-fraud.html

Adeoti, J. O. (2011). Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out. *Journal of Social Sciences*, *27*(1), 53-58.

Adomi, E. E. (2008). Combating cybercrime in Nigeria. *The Electronic library*, 716-725.

Affairs, O. o. (2015, july Monday). Retrieved from TheUnited States Department of Justice: http://www.justice.gov/opa/pr/six-nigerian-nationals-extradited-south-africa-mississippi-face-fraud-charges

Aina, A. (2008). The Internet and Emergency of Yahoo boys sub Culture in Nigeri. *International journal of Cyber Criminology*, 368-381.

Allison, S. F. (2003). *A case study of identity theft* (Doctoral dissertation, University of South Florida).

Aliyu, O. T. (2011). Social Organization of Internet Fraud among University graduates in Nigeria. *Cyber crime journal*, 860-875

Anderson, D. S., Fleizach, C., Savage, S., & Voelker, G. M. (2007, August). Spam scatter: Characterizing internet scam hosting infrastructure. In *Usenix Security* (pp. 1-14).

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer Berlin Heidelberg.

Antes, J., Conley, J., Morris, R., Schossow, S., Yee, Z., & Fang, F. (2008). Cyber Crimes: Real Life and in the Virtual World.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyber psychology, Behavior, and Social Networking*, *14*(12), 759-763.

Azeez, N. A., Iyamu, T., & Venter, I. M. (2011). Grid security loopholes with proposed countermeasures. In *Computer and Information Sciences II* (pp. 411-418). Springer London.

Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa—Cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, *11*(2), 85-100.

Bocij, P. (2006). *The dark side of the Internet: protecting yourself and your family from online criminals*. Greenwood Publishing Group.

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*, *32*(5), 477-493.

Burrell, J. (2008). Problematic empowerment: West African Internet scams as strategic misrepresentation. *Information Technologies & International Development*, *4*(4), pp-15.

Brunton, F. (2013, May 19). *Boston Globe*. Retrieved from https://www.bostonglobe.com/ideas/2013/05/18/the-long-weird-history-nigerian-mail-scam/C8bIhwQSVoygYtrlxsJTlJ/story.html

Chawki, M. (2009). Nigeria tackles advance free fraud. *J. Inf. Law Technol*, *1*(1), 1-20.

Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.

Cohen, A. K. (1955). Delinquent Boys; The Culture of the Gang.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review,* 588-608.

Duah, F. R. A. N. C. I. S. C. A. (2013). *Growing Global Threat of Cyber Crime: Implications for International Relations* (Doctoral dissertation, University of Ghana).

E.E, A. (2008). *Security and software for cyber cafes.* Ibadan: Emerald group publishing limited.

E.JOSEPH, A. (2006, june 28). *Cybercrime definition*. Retrieved from Computer Crime Research Center: http://www.crime-research.org/articles/joseph06/

Ebenezer, J. A. Cyber Fraud, Global Trade And Youth Crime Burden: Nigerian Experience.

Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal-January*, 93-98.

Ejiofor, C. (2015). Retrieved from Naij.com: https://www.naij.com/68635.html

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, *8*(4), 389-406.

Freeman, C. (2016, 02 05). Retrieved from The Telegraph: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/nigeria/12143510/Nigerians-reputation-for-crime-has-made-them-unwelcome-in-Britain-says-countrys-president.html

Fried, R. B. (2001). Cyber scam artists: a new kind of. con. *Crime scene investigator network*.

Goutam, R. K., & Verma, D. K. (2015). Top Five Cyber Frauds. *International Journal of Computer Applications*, *119*(7).

Hastings, D. (2014, february 4). www.nydailynews.com. Retrieved from Daily News: http://www.nydailynews.com/news/world/nigerian-man-arrested-case-dead-australian-widow-article-1.1601806

Hees, B. v. (2015, September 8). Nigerian jailed for online dating scam. Retrieved from iOL: http://www.iol.co.za/news/crime-courts/nigerian-jailed-for-online-dating-scam-1912847

Higgins, G. E. (2010). *Cybercrime: An introduction to an emerging phenomenon* (p. 3). McGraw-Hill Higher Education.

Igwe, C. N. (2007). *Taking Back Nigeria from 419: What to Do about the Worldwide E-mail Scam--advance-fee Fraud*. iUniverse.

International Mass-Marketing Fraud Working Group. (2010). Mass-marketing Fraud: A Threat Assessment.

Keyser, M. (2001). *Explanatory Report to the convention on cyber crime.* Budapest: European treaty series

Koong, K. S., Liu, L. C., & Wei, J. (2012). An examination of Internet fraud occurrences. *Retrieved on 15th July*.

Kshetri, N. (2006). The simple economics of cybercrimes. *Security & Privacy, IEEE*, *4*(1), 33-39.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly*, *31*(7), 1057-1079.

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

Longe, O. B., & Chiemeke, S. C. (2008). Cyber Crime and Criminality in Nigeria: What Roles Are Internet Access Points in Playing?

LONGE, O. B., CHIEMEKE, S. C., ONIFADE, O. F. W., & Longe, F. A. (2009). Camouflages and Token Manipulations-The Changing Faces of the Nigerian Fraudulent 419 Spammers. *African Journal of Information & Communication Technology*, *4*(3), 12.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, *9*(3), 155-172.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, *9*(3), 155-172.

McGuire, M., & Dowling, S. (2013). Chapter 2: Cyber-enabled crimes—fraud and theft. *Cybercrime: A review of the evidence*.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*.

McQuade, S. C. (2008). *Encyclopedia of cybercrime*. Greenwood Press.

Nakamura, L. (2013). *Cybertypes: Race, ethnicity, and identity on the Internet*. Routledge.

Newman, G., & McNally, M. M. (2005). *Identity theft literature review*. Washington, DC: National Institute of Justice.

Ngo-Ye, T. (2013). Stress from Internet Fraud and Online Social Support. *Stress*, *5*, 18-2013.

Ogwezzy, M. C. (2012). Cyber Crime and the Proliferation of Yahoo Addicts in Nigeria. *AGORA Int'l J. Jurid. Sci.*, 86.

Ojedokun, A. A. (2005). The evolving sophistication of Internet abuses in Africa. *The International Information & Library Review*, *37*(1), 11-17.

Okeshola, F. B., & Abimbola, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state of Nigeria. *American International Journal of Contemporary Research, 3*(9), 98-114.

Olugbodi, K. (2010). Fighting Cyber Crime in Nigeria. Retrieved September 10, 2011 from http. *www. guide2nigeria, com/news_articles_About_ Nigeria*.

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Cybercrimes and cyber laws in Nigeria. *The International Journal of Engineering and Science (IJES), 2*(4), 19-25.

Oriola, T. A. (2005). Advance fee fraud on the Internet: Nigeria's regulatory response. *Computer Law & Security Review, 21*(3), 237-248.

Oyesanya, F. (2005, *May 25*). Nigerian Internet 419 on the loose. *Retrieved from* http://www.nigeriavillagesquare.com/articles/nigerian-internet-419-on-the-loose.html

Oyesanya, F. (2004, March 28). Nigerian Internet on the loose. Retrieved from http://www.nigeriavillagesquare.com/articles/nigerian-internet-419-on-the-loose.html

PA, M. L. A. B., CATILOGO, P. A. C., & DEL ROSARIO, P. E. M. the incidence of cybercrime among youth social network sites users. *Editor's Note*, 62.

Park, W. Digital Jewels," The 2014 Nigerian Cyber Threat Barometer Report," 2014.

Peel, M. (2006). *Nigeria-related financial crime and its links with Britain*. London: Chatham House.

Premium times. (2016, January Sunday). Retrieved from http://www.premiumtimesng.com/news/165608-police-nab-first-class-honours-graduate-others-over-internet-fraud.html

Reich, P. C. (2008). Cybercrime, Cybersecurity, and Financial Institutions Worldwide.

Ribadu, N. (2004). Obstacles to effective prosecution of corrupt practices and financial crime cases in Nigeria. *House of Representative Committee on anti-corruption, national ethic and values, Kaduna, November, 2324.*

Robins, A. (2010). Prevent, protect, pursue – a paradigm for preventing fraud. *Computer fraud and security*, 5-11.

Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation.

Saulawa, M. A. A., & Abubakar, M. K. (2004). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. *Economic Times*, 1.

Scam Watch. (2015, December). Retrieved from SCAMWATCH.COM: https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

Singh, R., Singh, P., & Parveen, F. Cyber Crimes: The Rampaging Threat.

Smith, R. (2010). Identity theft and fraud. *The Handbook of Internet Crime. Devon: Willan Publishing*, 273-301.

Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). *Nigerian advance fee fraud*. Canberra: Australian Institute of Criminology.

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of criminology*. Rowman & Littlefield.

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860.

Van De Walle, N., & Smith, D. J. (2007). A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria.

Vanguard Nigeria. (2010, October 27). Retrieved from http://www.vanguardngr.com/2010/10/internet-13-years-of-growth-from-ground-zero-in-nigeria-from-1960-1996

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.

Whitty, M. T., & Buchanan, T. (2012). The Psychology of the Online Dating Romance Scam. A Report for the ESRC. *available online at www2. le. ac. uk/departments/media/people/monica-whitty/Whitty_romance_scam_report. pdf*.

Yar, M. (2013). *Cybercrime and society*. Sage.