# Social Media Users Opinion on Facebook and Email Frauds: A Study of the Students of Kaduna State University, Nigeria

**Mainasara Yakubu Kurfi, Ph.D**
**Department of Mass Communication**
**Bayero University, Kano, Nigeria**
mykurfi@gmail.com

**Abstract**

*The development of social media was brought by Information and Communication Technology leading to gradual disappearance of boundaries and turning the entire world into connected communities in what is usually described as 'global village'. As global communities get more connected, there are benefits and drawbacks. One of such drawbacks is that fraudsters and scammers who utilize the global connectedness to deceive innocent online users through all sorts of cyber-crime activities. This unhealthy activity has attracted global concerns and opinions. This paper examined opinion of students of Kaduna State University, Nigeria, on Facebook and Email Frauds. Survey method was used to investigate the subject matter. Using purposive sampling technique, a total of two hundred (200) respondents were drawn from the undergraduate of the University. Findings revealed that, frauds on social media take place by sending scam messages via email accounts or posting messages tagging the victims requesting for their Bank Verification Number (BVN) so as verify bank account of the unsuspecting use and sometimes hacking of Facebook or email accounts and then sending threatening messages containing false information subjecting the account users being duped. The study further found that these frauds are attributed to lack of employment, poverty and laziness among youths. The study recommends that the public especially online users should constantly be sensitized on cyber frauds to avoid being scammed.*

**Key words:** Online Fraud, Facebook, Email, Social Media, Kaduna State

## Introduction

The use of social media to communicate among different people in the contemporary world has indeed come to stay. This is because social media is a pretty nifty tool for keeping in touch to a large number of heterogeneous audiences within the shortest possible time. Platforms such as Facebook, email, Twitter, Instagram and WhatsApp among others offer users variety of ways in which they can remain connected at all times. However, the seemingly endless capacity for sharing, swiping, liking and retweeting has some negative consequences, not the least of which is that it opens users up as targets for online frauds. Some of the social media disadvantages are the emergence of online fraud perpetrated by some dubious characters. For instance, they "hijack" users' accounts, identity theft, impersonate Facebook security or administrator among others. These hijacked social media accounts would then be used to send fake messages to other

users, warning them that their account was about to be disabled and instructing the users to click on a link to verify their account. The users would be directed to a false Facebook page which often ask them to enter their login info and their credit card information to secure their account. This is one of the several ploys deployed by scammers, even as the social media users continue to grow numerically.

Global Internet Users (2017) reported that the number of Internet users across the globe has reached 3,739,698,500 as at March 2017. Considering this figure, online activities will certainly continue to increase dramatically and individuals will continue to use the Internet for a variety of purposes including email, chat, research, video communication, online banking, electronic commerce and online auctions. As such, careless, ignorant and unsecured online users on Facebook or emails are vulnerable to hackers and scammers who pretend to offer mostly financial assistance. These hackers and scammers are arguably believed to be smart in understanding the perceptions and expectations of online users they are targeting to defraud.

Nigerians like other nationals are active users of various social media platforms. The unimaginable internet penetration has brought online activities more closely than ever to Nigerians as a result of the emergence of mobile internet services. Nigerian Communications Commission (NCC) report showed that the number of internet users in Nigeria's telecommunications networks increased to 91.6 million in June, 2017 (The Sun, 2017). This development has spurred a growing number of social media users in Nigeria. NCC noted that there is an increasing volume of information shared on platforms such as Facebook, Twitter, WhatsApp, Blackberry Messenger and Instagram, to mention just a few among several social media networks through which Nigerians interact, obtain information to meet their social needs. It revealed that over 16 million Nigerians are on Facebook, the highest in Africa, making Nigerians the most active users in the continent (omojuwa.com, 2017). This development indicates that Nigerians are obviously among the millions of global social media users prone to online fraud or scam.

There are several media reports of Nigerians of all ages falling victims or perpetrators of the online scam or fraud. They wreak the live of other Nigerians and foreigners through the advance fee fraud running into millions of Naira, Dollars, Pounds Sterling and Euros (Gabriel, 2015). According to Gabriel (2015) "whether they call it 419, Obtaining By Trick, OBT or Yahoo-Yahoo, it is the same story. People are using the internet to perpetrate scams that deprive many of their hard earned money, destroy businesses and make nonsense of their lives".

Studies have revealed that many people (email and Social Media users) especially youths are victims of such frauds which in one way or the other has affected their lives (Button et al.; Ngo-Ye, 2013; Idolor, 2012; Graziolo and Jarvenpaa, 2003; Nikitkov and Bay, 2008).

However, most of these studies focused on the nature of such scams, modalities, business or corporate organizations that have fallen victims but, much has not been documented on the opinions of users especially among youths who are the largest

category of users of these social media platforms (Duggan, 2015). This study fills a gap in knowledge by examining the opinion of youths in the higher institution who constitute the large number of social media users – a platform used by the cyber fraudsters, thus placing the youths as more vulnerable group. The study therefore attempts to achieve the following objectives:

- To find out whether undergraduate students of Kaduna State University have ever received suspected fraud message(s) on Facebook/email
- To find out their reaction to fraud message(s) on Facebook and email
- To find out their opinion on the reasons for Facebook and Email Fraud
- To identify the different forms of frauds on Facebook and in emails that takes place in the context of undergraduate students of Kaduna State University

**Literature Review**

Duffield and Grabosky (2001) described online fraud as an act involving deceit (such as intentional distortion of the truth or misrepresentation or concealment of a material fact) to gain an unfair advantage over another in order to secure something of value or deprive another of a right.

The term 'online fraud' refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme (AFP, n.d)

According to Gabriel (2015) online fraud is tagged differently in different countries. For example in Nigeria it is referred to as 419, Obtaining By Trick, OBT or Yahoo-Yahoo with People are using the internet to perpetrate scams that deprive many of their hard earned money, destroy businesses and make nonsense of their lives. Boudonck (2017) noted that these online scams are developed daily. The scammers use old scams with new twists, thus further making every user vulnerable.

The online platforms have generated in recent times several ways of defrauding users. In Internet users everyday face various forms of scams and frauds online. Boudonck (2017) pointed out that it has been common in recent times to especially on Facebook; scammers are copying the profile of other users and then contacting their friends and family asking for money Several media reports surface daily on how internet users across the globe encounter these scammers and how they have lost possessions, especially money. These scammers of all ages who wreak the lives of other internet users and through the advance fee fraud running into millions of Dollars, Pounds Sterling and Euros (Gabriel, 2015) Gabriel (2015) noted that Scammers have developed new ways to try to convince people that their money-grubbing cons are really genuine. Nigerians are duped everyday through business and love scams. Foreigners are the worse victims. On weekly, nay daily basis, new variations of the so-called Nigerian 419 scam (named for the section of the Nigerian constitution that deals with this crime) appear.

AFP (n.d.) identified forms of online fraud such as:

- Internet banking fraud (Internet banking fraud is fraud or theft committed using online technology to illegally remove money from, or transfer it to, a different bank account.) Phishing (Phishing involves using a form of spam to fraudulently gain access to people's internet banking details using of spam e-mails purporting to be from a bank, in this way criminals 'fish' for legitimate bank customer's logon information.)
- Mule Recruitment (criminals advertise jobs on popular employment or job-seeking websites, online in chat rooms or through unsolicited employment emails.)
- Shopping and auction site fraud
- Spam (sending unsolicited commercial messages sent via email, SMS, MMS and other, similar electronic messaging media trying to persuade users to buy a product or service, or visit a website attempting to trick you into divulging your bank account or credit card details.)
- Identity theft: This can include the theft and use of identifying personal information of persons either living or dead.

Nikitkov and Bay (2008) examined shill bidding (a form of internet fraud where a seller enters a bid on his/her own item) to illustrate the ethical and legal issues related to internet fraud. The study was carried out using a systematic analysis of the rate of shill bidding occurrence on eBay, transaction data were gathered from the history of bids web pages maintained by eBay. The finding of the study disclosed that the rate of shill bidding is relatively high, much higher than the 0.1% estimated by eBay (18% for motor category, 15% for computers, and 28% for beauty category). Given the magnitude of internet fraud, the study suggested that it is likely that controls will have to be instituted, e.g. governmental, code based, user initiated or instituted by the firm.

Button et al. (n. d.) edited a compendium of works on "*Fraud Typologies and Victims of Fraud*". Their work examines wide range of online frauds which affect individuals and corporate organizations. It highlights the diversity within fraud including who perpetrates it and the level of innovation and skill involved in committing fraud, thus coining the word 'scampreneurs' to describe these criminals. The report found that there are wide ranges of techniques used to commit frauds, which can be divided into four areas: first, *victim selection techniques;* second, *perpetration strategies*; third, *detection avoiding strategies*; and fourth, *securing the gains*. The report also classified online fraud into: *Internet matrix scams* where the scammers operate via online adverts offering free gifts; *Internet dialer scams* where fraudsters send out emails or create pop up boxes on websites, which when downloaded or clicked upon downloads software that changes their Internet settings and *African advanced fee frauds*, here fraudsters use mail, e-mail or faxes to target potential victims with usually a fictitious scenario of a corrupt government official who has 'procured' large sum money and who needs a bank account to place it.

Ngo-Ye (2013)'s *Stress from Internet Fraud and Online Social Support* is another study which investigated ordinary user's response to internet transaction fraud and examining the types of online social support. The study adapted the stress process model from the psychological literature and applied it to the context of internet fraud. Using qualitative case study (in-depth interviews with the victims belief, emotion and behavior response to a fraud and discussions on eBay Community Answer Centre, the study found two types of support mechanisms – the factual information exchange and emotional support.

Similarly, a new whitepaper from antivirus company – *Bitdefender*, conducted a study titled "*Users Can't Tell Facebook from a Scam*" which examined 850,000 Facebook frauds spreading in countries such as the US, the UK, Australia, Germany, Spain, France and Saudi Arabia for over two years, showing the psychology of those who get taken in and how Facebook's own user experience enables these scams to flourish. The study found that scammers have infected millions of users with the same tricks over and over again. Concluding that Facebook's user experience makes it easy for scammers to exploit them and that users falling for Facebook scams are simply falling for their expectation of Facebook's users experience (Blue, 2014).

Dobovsek et al (2013)'s *Advanced Fee Fraud Messages on Facebook – Non declining Trend* investigates some intake on advanced fee frauds using qualitative analysis from 1998 – 2015 by analyzing 547 related messages on emails. The study found that advanced fee frauds are not declining in occurrence. They are consistently developing and use both bulk sending and narrower settings. Also, the study discovered that there seems to be a severe resemblance and connection to other types of frauds, especially online frauds such as pilfering, phising or email spoofing. These types of frauds are globally and no country is immune from hosting the perpetrators.

A study conducted by Google in conjunction with the University of California, San Diego (UCSD), email scams are more effective than imagined. The study examined 100 phishing emails picked out of a random sample self-reported by Gmail users. It also reviewed a random sample of 100 phishing websites caught by *Google's Safe Browsing* system to further understand how the scams work. These websites were all created through Google Forms, which is how researchers were able to access the data. One of the findings of the study indicates that once on the bogus pages – which tend to imitate legitimate sites, like Google itself, in an effort to obtain people's private details – 14 percent of people unwittingly submit their information to hackers. Also, the study found that even on the worst-performing phishing websites, 3 percent of users still submitted their data. On the most effective phishing sites as many as 45 percent did. The study concludes that hackers use Gmail's own search function to figure out if an account is worth their time, looking for terms like "wire transfer" and "bank." At the end, it recommends that online users should enable two-step verification on their email accounts, and report any suspicious emails instead of responding to it (Beres, 2014).

A number of studies from Nigeria's perspectives have been carried out by many scholars, some of these studies include the work of Hamilton et al. (2010)'s *Dimensions of fraud in Nigeria Quoted Firms*. The study examined the management of financial fraud in quoted companies in Nigeria using a sample size of 22 firms through administration of questionnaires and in-depth interviews methods. Some of the findings of the study are that; poor internal systems are the major cause of frauds in Nigerian organizations; funds diversion is the commonest kind of fraud; most business organizations do not make fraud cases public; young people within the age of 31-40 years and polygamists recorded highest cases of involvement in fraudulent acts among employees; and finally the frequency of males involvement in fraudulent act surpassed that of females. The study concludes that even though fraud cannot be completely eliminated from business life, its occurrence can be minimized through better internal control systems.

Tope (2012)'s Patterns of Internet Security in Nigeria: An Analysis of Data Mining, Fraud Detection and Mobile Telecommunications in Unsupervised Neutral Networks is another study with Nigeria's perspective. The study examined the relationship between data mining and internet security in Nigeria using *MTN*, *Glo*, *Airtel*, *Etisalat*, *Multilinks*, *Starcomms* and *Visafone* as leading telecommunication service providers as the case study. The study used survey method through administration of two hundred questionnaires to the undergraduate students of Lagos State University, Ojo. The study found that online fraudsters popularly known as "yahoo boys" in Nigerian context take advantage of ecommerce system available on the Internet to defraud unsuspected victims who are mostly foreigners. They persuade them through offers such as free browsing, free international call and free text messaging among others. Others defraud individuals through the use of social media such as Facebook, twitter, tafoo, myspace, and yahoo chat. The study concludes that there is a correlation between data mining and fraud detection in unsupervised neural networks in that the former helps in improving security in the country.

These internet or online frauds come in various forms, such as somebody is using your email account to solicit funds from your Facebook friends, your colleagues or other contacts in your email. Another form is receiving text or email messages from unknown sources informing you of an inheritance you don't know about being paid into your bank account and leaving a number for you to contact for details that could lead to maximizing the benefits of that inheritance and before you know it, people are duped! It could also be a text or email message informing you about winning a lottery you never entered into or using things they think you are familiar with to hoodwink you! Sometimes too, it could be a rich married woman being lured into a love web with the motive to dupe her of her resources or that of her husband via blackmail whether the love scene is real or make-believe (Gabriel, 2015).

Other forms include hacking into Facebook accounts, then sending messages to all the listed friends claiming the account owner is in trouble and asking for cash to be wired for their rescue; collecting names and email addresses of people who leave

messages on obituary site guest books and contacting them with a request for money, supposedly on behalf of the bereaved person; sending complimentary messages to bloggers and article authors (both online and in print) as a way of establishing a friendship that, sooner or later, results in a cash-call attached to a tale of woe; offering to buy your Internet domain name, then asking you to visit a site (their site) where you have to pay to have it valued; and using Microsoft Word documents as attachments. These contain details of the scam story but, because they are not in the main body of the email, they often don't get picked up by scam detectors in your security software (Gabriel, 2015, Boudnock, 2017).

To sum up, it can be argued that social media platforms have their respective advantages and disadvantages. It is clear from the previous studies that hackers used advantages of online users who are gullible in exposing their identities to those hackers. Many studies have established that online frauds take place across the globe using different tricks and techniques with a view to take advantage of online users.

**Theoretical Framework**

This study adopts the Rational Choice theories (RCTs) and Routine Activities theory. According to Akers (1990) The RCTs have a long history in disciplines such economics, sociology, political science, and criminology. However, many of the RCTs in different disciplines share a common core assumption on which the specific theory rests. Rational Choice Theory posits that offenders are rational people who weigh the benefits of engaging in a particular criminal behaviour against the risks associated with that behaviour (McQuade, 2006). Individuals have complete knowledge about their decision alternatives, the probabilities of their outcomes, and their consequences. Looking at this from the online scammers, they are outcomes and consequences of their actions but yet indulge in defrauding internet users and usually have preferences ranging from selfishness, opportunism, egoism, and linked-utility to solidarity. A selfishness assumption, for example, implies an individual will readily break rules (e.g., cheat) to maximize his or her benefits. In most RCTs, individuals are regarded as self-interested agents with the ability to make judgments about achieving subjectively defined goals (Akers 1990). For their selfish reasons they defraud users of various internet platforms.

The Routine activities theory puts forth that crimes happen when motivated offenders come in contact with suitable targets under a lack of capable guardianship (McQuade, 2006) this is the case in respect of online fraud. Scammers are usually motivated when they come across ignorant or careless internet users. Routine Activities further posits that three factors, increase victimization risk: 1. exposure to offenders, 2. deviant behaviour, and 3. target attractiveness while the presence of guardianship acts as a protective factor (Spano & Frielich, 2009). Facebook and Email fraud victimization risk increases because the users are exposed to scammers and for selfish reasons the scammers harbour deviant behaviours and are attracted to users attractiveness. The more users engage in internet activities the more they expose themselves to potential scammers and are likely to fall victims of Facebook and Email especially if the lack guidance.

## Method

This study employed survey research method. A sample of two hundred (200) respondents was drawn from over seven thousand (7000) undergraduate students of Kaduna State University (KASU) registered for 2016/2017 Academic Session (Academic Division, Kaduna State University, 2017). The study used purposive sampling techniques for selecting the 200 respondents. The purposive sampling criterion for selection was those who have Facebook and Email accounts irrespective of the students' level of study, faculty or department. The study also used questionnaire as instrument of data collection. 200 questionnaires were self-administered, retrieved and found usable.

## Results and Discussions

### Gender of Respondents

On the respondent's demography, only 2 variables are relevant to the study which is respondents' age and gender. The findings revealed that 85% (n=170) of the respondents were between the ages of 18 - 25, 10% (n=20) were between 26 - 30 and 5% (n=10) respondents were between 41 - 45 years respectively. This shows that most of the respondents were between the ages of 18 – 25 years and hence within the range of youthful age as a concern of the study. On the respondents gender, the data shows that 54% (n=108) of the respondents were male while 46% (n=92) were female students. This demonstrates that majority of the respondents who answered the questionnaires were females hence showed a degree of equal representation of both sex.

### Ownership of Facebook and Email Accounts

On use of social media, the study found that all the 200 (100%) respondents have email address. 175 respondents (87.5%) confirmed that they have Facebook accounts, while 25 (12.5%) respondents do not have Facebook accounts. This also indicates that majority of the respondents have account with both Facebook and email address which they have been operating within the range of 1 to 10 years.

Table 1 showing whether the respondents have ever received suspected fraud message(s) on Facebook/email

| Answer | Frequency | Percentage |
|---|---|---|
| Yes | 147 | 73.5% |
| No | 53 | 26.5% |
| Total | 200 | 100% |

The table above shows that 147 (73.5%) respondents have received messages suspected to be online frauds on their Facebook accounts and or emails addresses. While 53 (26.5%) respondents indicated that they have never received such messages. This means that majority of the respondents have in one way or the other been exposed to scam messages on either Facebook or in their emails by make believe who posed to offer mostly financial assistance but ended up duping their victims.

**Reaction of respondents to Facebook and Email Fraud Messages**

A follow up question on how they reacted to such messages for those who received it found that 92 (46%) respondents ignored such messages; 12 (6%) replied to those fraud messages; 8 (4%) respondents used to warn the senders of such messages to desist from sending same messages to them in the future, while 35 (17.5%) respondents confirmed that they blocked the senders of such messages from their respective Facebook accounts. In view of the above, the result showed that majority of the respondents who have Facebook and email have encountered cyber fraud and hence validate the fact that the social media users are vulnerable to such crimes.

**Idea on Forms Fraud Messages**

Those who admitted that they have an idea, their answers revealed The forms and nature of fraud messages include :sending fraud messages via email accounts or posting messages tagging the victims requesting for their Bank Verification Number (BVN) for verification in case of bank accounts and sometimes hacking of Facebook or email accounts and then sending threatening messages containing false information subjecting the account users to duping as how frauds usually take place on social media.

**Respondent's Opinion on the reasons for Facebook and Email Frauds**

In an open-ended question on the reason(s) why these frauds take place, majority of the respondents attributed the act to unemployment particularly among teeming youths who graduated from colleges and universities without employment. Some respondents stated poverty and laziness among youths as influencing factors that pave the way for the perpetrators to embark on online frauds.

Furthermore respondents are of the opinion that Facebook and Email frauds are illegal but easy money making venture for some youths.

**Forms or Nature of Facebook and email Frauds**

On the form or nature of these online frauds, some of the respondents were of the view that the form of Facebook and email frauds come in form of business offer, seeking for bank personal information, job opportunities and scholarship offer to the potential victims. They also revealed that some of the victims were tricked in sharing their personal information with the fraudster who turned to dupe them at the end of the interaction.

Respondents further revealed that the frauds take the forms of:

- sending fraud messages via email accounts or
- posting messages tagging the victims requesting for their Bank Verification Number (BVN) for verification in case of bank accounts and
- sometimes hacking of Facebook or email accounts and then sending threatening messages containing false information subjecting the account users to being duped

On the best preventive measures to avert being duped, the respondents mentioned ways as thus: ignoring the kinds of message, blocking the senders of these messages or reporting them to the appropriate authorities and proper screening of friend request on Facebook.

**Conclusion/Recommendations**

The paper examined opinion of the students of Kaduna State University, Nigeria on Facebook and email fraud. From the findings of the study, the paper concludes that people who have Facebook and email accounts have in one way or the other been exposed to scam messages by scammers who pretend to offer financial assistance. As such social media users are vulnerable to such crimes. This is in tandem with Boudonck (2017)'s findings who maintained that it has been common in recent times especially on Facebook where scammers are copying the profile of other users and then contacting their friends and family asking for money. Usually, frauds take place on social media by sending scam messages via email accounts or posting messages tagging the victims requesting for their Bank Verification Number (BVN) for verification in case of bank accounts and sometimes hacking of Facebook or email accounts and then sending threatening messages containing false information subjecting the account users to duping. This finding related to Button et al. (n. d.) findings on "*Fraud Typologies and Victims of Fraud*" where they discovered the following types of online frauds: Internet matrix scams, Internet dialer scams and African advanced fee frauds. Unemployment among youths who graduated from colleges and universities without employment has been described as one of the causative factors. Also, poverty and laziness among youths pave the way for the perpetrators to embark on online frauds. It has been established that Facebook and email frauds are illegal but easy money making among jobless youths.

This is the social reality constructed by the frauds. The different strategies or forms used by perpetrators vary according to the specific type of fraud but some of the most common include stealing of victims' personal information through hacking, offer of business, update for latest technology, promotion of products and services, and seeking for some amount of money among others. This therefore validates Duffield and Grabosky (2001) submission that online fraud involves intentional distortion of the truth or misrepresentation or concealment of fact with the aim of gaining advantage over another. To conclude, the study argues that there is a strong correlation between the findings of this study and other studies reviewed in the paper.

In view of the above findings, the paper wishes to recommend that:

- The general public especially online users should constantly be sensitized on cyber frauds to avoid victimization of users as well as the general public.
- Online users should be cautious in accepting request from strange person(s) as acceptance of such request subject users to be vulnerable to fraud.
- Use of strong passwords and different passwords for different platforms should be encouraged among users as having one password for many platforms exposes users to this kind of risk.
- "Http" links should be used on email accounts to ensure only one person access to personal conversations. Update software and dives from genuine applications only.
- Do not share login info, not even with people you trust. Close friends and family might still accidentally make you vulnerable if they are using your account.
- Make use of any security settings offered by social media platforms. Examples of these include privacy settings, captcha puzzles and warning pages informing you that you are being redirected offsite.

**References**

Akers, L. 1990, "Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken," (81:3), pp. 653-676.

Australian Federal Police(AFP) (n.d.) Online fraud and scams. Retrieved from https://www.afp.gov.au/what-we-do/crime-types/cybercrime/online-fraud-and-scams

Beres, D. (2014). "Google Study Finds Email Scams Are More Effective Than You'd Expect". *The Huffington Post*. Retrieved from: www.huffingtonpost.com/2014/11/07/phishing- scams_n...

Blue, V. (2014). *A Review of Literature on Types of Fraud and Trust Building: A Monograph*. Retrieved from: http://dx.doi.org/10.4337/9781848445086.00014

Boudonck, C. (2017) Top 25 ways of avoiding scams online. *OnlineMLMCommunity*. Retrieved from https://onlinemlmcommunity.com/avoid-scams-online/#respond

Button, M., Lewis, C. and Topley, J. (undated). *Fraud typologies and victims of frauds: literature review*. National Fraud Authority. Centre for Counter Fraud Studies, Institute of Criminal Justice, University of Portsmouth.

Dobovsek, et al (2013). "Advanced Fee Frauds Messages on Facebook – Non-declining Trend". *Journal of Money Laundering Control*. Vol. 16, Number 3, Emerald Group Publishing Limited.

Duffield, G., Grabosky, P. (2001). The psychology of fraud. Trends and issues in crime and criminal justice 200. *Australian Institute of Criminology*, Canberra.

Duggan, M (2015) The Demographics of Social Media Users. Pew Research Center. Retrieved from http://www.pewinternet.org/author/mduggan/

Gabriel, C. (24 January, 2015) 419: The world of the Nigerian fraudster. *Vanguard Newspaper*. Retrieved from http://www.vanguardngr.com/2015/01/419-world-nigerian-fraudster/

Grazioli, S., Jarvenpaa, S. (2003). Deceived! Under target online. *Communications of the ACM*, *46*(12), 2003, 196-205.

Hamilton, D. I., Justin, M. and Gabriel, O. (2012). *Dimensions of fraud in Nigeria quoted firms*. American Journal of Social and Management Sciences. Retrieved from: http://www.scihub.org/AJSMS.

Internet World Stats (2017) Global Internet Users. *World Internet Stats*. Retrieved from http://www.internetworldstats.com/stats.htm

McQuade, S. (2006). Understanding and Managing Cyber crime. Boston, MA: Pearson Education Inc.

Nikitkov, A., Bay, D. (2008). Online auction fraud: ethical perspective. *Journal of Business Ethics*, *79*(3), 235-244.

Ngo-ye, T. (2013). *Stress from Internet fraud and online social support: proceedings of the Southern Association for Information Systems conference*, Savannah, GA, Dalton State University, USA March 8th–9th, 2013, p. 168.

Omojuwa.com (June, 2017) Nigeria has the highest number of Facebook users in Africa – NCC. Retrieved from http://omojuwa.com/2017/06/nigeria-highest-number-facebook-users- africa-ncc/

Spano, R. and Frielich, J.D. (2009). An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005. Journal of Criminal Justice, 37(3), 305-314.

The Sun (July 27, 2017) Nigeria's internet users rise to 91.6m. *The Sun Newspaper* Retrieved from http://sunnewsonline.com/nigerias-internet-users-rise-to-91-6m/

Tope, O. (2012). *Patterns of Internet Security in Nigeria: An Analysis of Data Mining, Frauds Detection and Mobile Telecommunications in Unsupervised Neutral Networks*. Retrieved from www.omotere.tk.