PATTERNS OF INTERNET FRAUD IN NIGERIA: IMPLICATIONS FOR VICTIMS

Nuhu Joseph Maigari
Economic and Financial Crimes Commission,
Abuja

Andrew Zamani
Institute of Governance
Nasarawa State University, Keffi

Udo Chikezie Osisiogu
Department of Sociology
Nasarawa State University Kefii

Abstract

This paper examines the criminal victimization patterns adopted by internet fraudsters in Nigeria and their implications for the victims. The paper relied on secondary sources of data such as journal articles, organizational and institutional publications, newspaper reports, and textbooks, among others. The rational choice theory was used to analyze the phenomenon examined. The patterns of victimization used by internet fraudsters include hacking, smartphone-based fraud, the use of malicious software or malware, cyber identity theft/phishing, website jacking/cloning, and software piracy. The paper concludes that internet fraudsters are clever, rational criminals that persist in using devious victimization patterns that allow them to outwit their targeted victims and reduce the likelihood of being apprehended and prosecuted, while subjecting the victims to dire implications. Among other things, the paper recommends that regular enlightenment programmes should be used to educate the general public on the schemes adopted by internet criminals to defraud them. Security agencies should train more experts in the detection of cybercrime and provide them with the required technological tools to work with.

Key words: Internet fraud; pattern; criminal victimization.

Introduction

The advent of the internet has significantly impacted communication and human transactional activities in the world (Manyika & Roxburgh, 2011). According to Dogruer, Eyyam, & Menevis (2011), on the internet, anyone may now quickly access any kind of information that can be used for social, educational, and recreational purposes. The World Wide Web was reported to have expanded substantially. The number of internet users globally has considerably increased from 2009 to 2019 (Ansar, et al. 2021). Surfing the internet for various purposes has become part of the daily activities of many people (Bansal, Bhargavan, & Sergio 2012). However, the use of the internet for both licit and illicit purposes has become widespread. Therefore, despite the enormous benefits that the internet offers, it also exposes users to the risks of criminal victimization. In other words, the internet provides an opportunity for fraudsters to defraud thousands of people at once, robbing people of their earnings and causing them emotional harm, as well as stealing the finances of corporations.

Fraud happens when someone deceives another to gain illicit advantages over them (Kavrestad, 2014). Scammers use software or online services to swindle millions of individuals. This involves deceiving victims into paying cash or disclosing private information. Therefore, internet fraud involves the deployment of the internet to commit fraud. Internet fraud is a worldwide crime. According to the House of Commons (2017), internet fraud is currently the most common type of crime in England and Wales, hurting victims both financially and emotionally. In the USA, the Federal Bureau of Investigation (2021) report shows that between 2016 and 2020, about 2,211,396 incidences of internet scams occurred in the USA. Similarly, according to Sahara Reporters (2022), the United States tops the list of countries with the highest incidences of internet fraud, while the United Kingdom and Canada rank second and third, respectively.

In Africa, there are also rampant cases of internet scams, which have resulted in the victimization of millions of people within and outside the continent. According to Kshetri (2019), Africa is one of the regions with the fastest rate of growth for internet scams. The author reports that in 2017 alone, the African continent lost $3.5 billion to cybercrime. He argued that the continent is home to scammers perpetrating cyberattacks on people across the world. In the same vein, Interpol (2022), in its report on global crime trends, stated that phishing and other online frauds were identified as the highest recent danger and the type of crime that is more likely to rise in frequency over the next three to five years in Africa. In Nigeria, internet scams abound. A lot of Nigerians

and foreigners have been victimized by Nigerian internet fraudsters. According to Ezea (2017), internet scams became widespread in Nigeria in the 2000s as a result of increased access to the internet. In 2020, the Federal Bureau of Investigation ranked Nigeria 16th among the countries most ravaged by internet fraud globally (The Cable, 2023). The report of Statista (2022) on the number of financial criminals arrested in Nigeria in 2019 is indicative of the enormity of internet fraud in Nigeria. The report shows that, for advance fee fraud, 337 women and 1700 men were detained in Nigeria in 2019. In addition, 73 women and 878 men were detained for cybercrimes. This indicates that males significantly outnumber females among those who have been arrested in Nigeria for financial and commercial offenses. In order to prevent, identify, prosecute, and punish internet fraudsters in Nigeria, the federal government of Nigeria introduced the Cybercrime Act.

In spite of the arrest of several cybercriminals in this regard over the years, numerous youths continue to commit the crime (Ezea, 2017). This indicates that the introduction of the Cybercrime Act has proved ineffective in deterring internet fraudsters. According to Mnunyi (2022), internet fraud victimization occurs in all cities in Nigeria, albeit to varying degrees. Understanding the manner in which internet fraudsters operate is key to taking steps to forestall victimization. Therefore, the objective of this paper is to examine the patterns of internet fraud in Nigeria and suggest ways of foreclosing victimization.

Conceptual clarification

Internet fraud

Internet fraud refers to the use of online tools and programs with internet connections to scam or exploit people. According to the Australian Federal Police [AFP] (2023), internet fraud broadly refers to cybercrime behavior that occurs online or via email, such as identity theft, phishing, and other hacking attempts intended to defraud people of their money. Millions of dollars' worth of fraud occurs annually as a result of internet scams that prey on people using online services. Additionally, as internet usage grows and cybercriminal tactics advance, the numbers keep rising (AFP, 2023). According to Dashora (2011), internet fraud is committed against people or businesses using the Internet, computers, smartphones, or other illegal activities that use computers as a tool, such as online gambling, pornography, phishing schemes, spam, junk e-mails, fraud, forgery, identity theft, cyberstalking, and so forth. Obtaining illegal access to a person's or an organization's computer networks, electronic information theft, denial of service assaults,

malware, harmful codes, e-mail bombing, data tampering, web jacking, internet time theft, Trojan attacks, and other tactics are also other means of committing internet fraud (Dashora, 2011).

Theoretical elucidation

The rational choice theory (RCT) posits that law violations occur as a result of careful thought and planning. Law violations are preceded by an analysis of the perceived benefits the offender stands to derive from violating the law, such as money, thrill, revenge, and entertainment. Also taken into consideration are situational factors such as the vulnerability or otherwise of the target and the effectiveness of law enforcement (Hechter, 1997). The rational offender assesses the risk of being arrested, the certainty of punishment, the accruable rewards of law violations, and the need to obtain such rewards. On the one hand, the commission of certain offenses is a product of personal choice made following evaluation of the information available to the individual. On the other hand, the decision to abstain from law violations is a product of the individual's perception that the reward associated with breaking the law is not commensurate with the associated punishment should the offender be apprehended.

According to RCT, law violations are offense- and offender-specific. It is offense-specific because offenders do not react the same way to all offenses (Siegel, 2005). For instance, the decision to kidnap for ransom would be influenced by an assessment of the likelihood of getting the expected sum of ransom for kidnapping the victim, the availability of facilities like a vehicle for the "operation", accommodation to keep the victim, and the likelihood that the offender will not be arrested. Crime or law-violating behaviour is offender-specific in the sense that offenders do not just engage in antisocial behaviour without first ensuring that they possess the wherewithal to "succeed" in committing the chosen offense. Taken into consideration by the potential offenders are their skills, motives, needs, and fears (Siegel, 2005). Distinguishing between crime and criminality, Siegel (2005) noted that crime is an event while criminality is a personality trait. According to him, offenders, on the one hand, do not break the law all the time; on the other hand, conformists may occasionally violate the law. Furthermore, opportunity is a key factor in law violations. In this regard, a highly motivated offender who is willing and ready to commit an offense may not commit the particular offense if the opportunity to do so is lacking. However, the availability of the opportunity to offend could result in law-abiding individuals violating the law.

RCT submits that offenders evaluate a number of factors, such as place, target's characteristics, and availability of means, before actually breaking the law. Regarding place, lawbreakers carefully select a place considered more conducive to breaking the law. This involves choosing a place with a lower risk of apprehension than a place where the risk of apprehension is higher. For instance, a place where security has been beefed up by the police is likely to experience fewer criminal activities than a place with a lower police presence. The vulnerability of targets is another factor. Offenders tend to choose targets that are not guarded. In other words, if the potential target is well protected, the calculating offender would perceive it as risky to attack or victimize them. More so, law-breaking behavior involves learning the techniques of law-breaking in order to reduce the risk of apprehension and its attendant prosecution. To forestall violations of the law, RCT submits that three factors are critical. These are: ensuring that potential targets are adequately guarded; controlling the means to commit crime; and adequate monitoring of potential offenders (Akers, 1990). Those who have the motivation to break the law would do so if they were not adequately policed. Individuals who are desperate may consider violating the law, but it takes people who are irrational to break the law if adequate policing is provided and punishment for offenders is certain. The decision to break the law would be checked by the threat of criminal prosecution. It is the fear of apprehension and subsequent punishment that would deter people from breaking the law. Generally, it is expected that the number of law violators will reduce if punishment for crime counterbalances the gain of law violations and if law enforcement is effective. Certainty of punishment influences would-be offenders' decisions to commit crimes. Increasing the certainty of arrest, conviction, and sanction for law violations has the capacity to reduce the rate at which people break the law. A motivated offender would understand that the punishment associated with the intended violation is greater than the expected benefits.

The prevalence of lawbreakers is therefore traceable to people's perceptions of poor policing. That is, the chances of apprehension are low, and punishment for those apprehended is neither certain nor severe. The certainty of an arrest is influenced by the extent of police presence. It is the responsibility of the police to effect arrests and subject offenders to formal prosecution for offenses committed (Abell, 2001). This implies that the inadequacy of police presence would adversely affect the certainty of arrest for a law violation. Therefore, an adequate number of police officers on the street would determine the likelihood that those who break the law are arrested. Specifically,

RCT holds that sanctions should be applied in such a way that known law violators will not choose law-violating behavior in the future. For instance, a traffic violator on whom sanctions were adequately applied may be deterred from further committing traffic offenses. From the standpoint of rational choice theory (RCT), internet fraud is a product of the perception that cybercriminals and would-be offenders have about it based on their analysis of factors such as benefits of engaging in cybercrime, likelihood of being apprehended, extent of law enforcement, and certainty of punishment for arrested criminals, among others. These factors shape how internet fraudsters perceive cybercrime, which in turn determine whether it is committed or not. Cybercriminals would perceive internet fraud as a rewarding act if there were benefits accruable from it that outweighed the likely punishment. The calculating would-be offender would contrast the expected benefits with the likelihood of getting arrested by law enforcement agents.

Perception of the law against Cybercrime as weak would encourage the prospective offender to commit cybercrime as a consequence of the minimal risk of apprehension. Conversely, the perception of certainty of arrest and prosecution has the potential to dissuade potential fraudsters from committing cybercrime. In other words, if it is certain that the criminal will be arrested and made to face the penalty that outweighs the benefit foreseen, the offense is unlikely to be committed by virtue of perceiving it as unprofitable. It could therefore be argued that there is a connection between perceptions of the nature of enforcement of the Cybercrime Act and the tendency to commit fraud. The internet environment would be defined as a safe place to violate the law if law enforcement is adjudged to be weak.

Methodology

This theoretical paper uses both analytical and descriptive methodologies. The paper solely relies on secondary data sources, which include newspaper reports, journal papers, textbooks, and institutional and organizational publications. Online databases served as the source of the data. The paper draws a conclusion from the point of view of the rational choice theory.

Patterns and Implications of Internet Fraud in Nigeria

Hacking

Hacking involves gaining authorized or unauthorized access to a system, either for non-criminal or criminal motivations (Hall & Watson, 2016). It could be motivated by legitimate purposes, such as attempting to obtain data to identify and solve a problem (Hall et al., 2016), or for illicit

purposes, such as defrauding gullible people (Urbas & Choo, 2008). The Economic Times (2023) averred that it is easy to believe that hackers are very intelligent and proficient with computers, adding that it takes more knowledge and skill to break into a security system than to build one. Criminal hacking involves gaining access to and manipulating computers belonging to other individuals without their consent (Denning, 2001). According to Aransiola and Asindemade (2011), hackers install multiple pieces of software that could be used to hack the computer of a victim. Thereafter, the fraudster can gain access to the personal information of the victim.

Hackers utilize computer operating system flaws and vulnerabilities to break into files and take critical information from a victim's device. According to Makeri (2017), it involves installing sneaky software on a computer and using it to accomplish the hacker's goal. The author narrated that many hackers also attempt to employ password-hacking tools to obtain access to targeted information. When internet users enter their password and user name as necessary while utilizing certain popular Internet services, password sniffers use the password hacking tool to nose them out. Hackers have the ability to import data onto a computer and can also secretly observe everything the user does on the computer. It is possible for a hacker to install multiple programs on a computer without the user being aware of them. These applications can be used to steal credit card details and other private data, including passwords (Thomas & Loader, 2000). The system or website of a company may also be hacked in order to obtain sensitive and confidential information about its long-term goals.

In Nigeria, many people and companies or organizations have fallen victim to hacking. According to George (2023), bank customers, companies, and public institutions lose billions of naira to criminal hackers every year due to weak cybersecurity. In 2021, the head of a ring that specialized in breaking into bank accounts and business organizations' servers was apprehended in Lagos State by the operatives of the Special Fraud Unit of the Nigeria Police (Police Special Fraud Unit [PSU], 2021). According to PSU (2021), the kingpin who demonstrated expertise in the internet milieu had defrauded bank customers to the tune of about ₦1.87 billion. According to the report by Okeh (2023), two members of a gang connected to the hacking of over one thousand (1000) bank accounts and transferring the monies of the victims were arrested by Lagos State police command in 2023. This development was a sequel to the petition submitted to the police by the United Bank for Africa, the report stated. In the same vein, Abiodun (2023) reported that in

February 2023, hackers transferred about ₦2.9 billion from Flutterwave accounts. Fraudsters also use personal details such as the Bank Verification Number (BVN) they got through hacking to create false bank accounts, which they use for fraudulent transactions (Ejike, 2023). Relatedly, Idris (2020) reported that the databases of two commercial banks were hacked. The leaked personal details of people in the said database included their names, addresses, phone numbers, email addresses, and dates of birth.

Hacking results in the stealing of the personal information of individual and corporate victims, subjecting them to a number of implications. For the individuals, the feeling of anxiety upon realizing that personal information has been lost can be disconcerting. This is due to the fear that the criminal would use such information to carry out damaging activities against the victim. Organizations whose websites or servers have been hacked would also suffer huge financial losses, as cybercriminals could divert funds and initiate other fraudulent transactions. Furthermore, it could result in the loss of organizational reputation, resulting in the public losing confidence in the organization. The loss of confidence could discourage the public from transacting any business with the organization or patronizing them for service rendering.

Smartphone-based Fraud

Internet fraudsters also target smartphone users. Any fraudulent behavior or illegal transaction carried out using a mobile device is referred to as mobile fraud. Common ways of perpetrating this kind of fraud include the circulation of fake smartphone applications by fraudsters. Such fake applications display advertisements for products and services that may appeal to the smartphone user. Payment for these products and services requires entering credit card details into the provided form. Upon supply of these details by the mobile phone user, they are stolen and used to steal the victim's money. The fake apps are also virus-infested, and downloading them puts the mobile phone owner at risk (Business Day, 2023). A cellphone virus has the ability to obtain information about individuals or demand money from those who are affected (Dunn, 2020). Mobile phone users who make use of public WiFi also stand a chance of being victimized. In this case, being connected to the same network that a fraudster is connected to may result in the fraudster redirecting unsuspecting people to a fake website where their personal data can be stolen.

It is concerning that mobile malware, which mostly targets Android smartphones, is becoming more prevalent. More than one in seven mobile devices in Nigeria is currently infected with mobile malware, according to Symantec (2016). Over 60% of fraud done online occurs on mobile

platforms, while 80% of fraud perpetrated on mobile devices occurs through mobile apps as opposed to mobile web browsers (Dunn, 2020). Similarly, Business Day (2023) reported that a recent survey conducted by the Financial Institutions Training Centre (FITC) found that the largest amount of money lost by Nigerian banks to fraud in the first quarter of 2023 was due to mobile fraud. The survey result indicates that in 2023, mobile fraud increased by N1.1 billion within the first three months of the year. This increase is higher than the N938 million recorded in the fourth quarter of 2022, by 18.3 percent, the study revealed (Business Day, 2023). Smartphone users are susceptible to victimization given the increasing extent of the use of mobile phones for financial transactions (Coony, 2012).

Considering that mobile phones are massively used in Nigeria by both literates and illiterates, mobile phone-based fraud is bound to be rampant, resulting in massive loss of savings. This is because cybercriminals do not relent in contacting unsuspecting mobile phone users to trick them into divulging the information that they need to defraud them. With the growing use of phones for financial transactions, the likelihood of mobile phone-based fraud is high.

Use of malicious software/malware

One of the patterns of internet fraud is the use of malware to steal the personal information of victims and then defraud them using the stolen information. Malware is an application or piece of software that is surreptitiously introduced into a system with the aim of jeopardizing the privacy, accessibility, or credibility of the individual's data, applications, or operating system. It is the term for software that hackers employ to breach a system, steal private data, corrupt data, interfere with computer functions, or access a network (Harvy, 2017). The Federal Trade Commission (2021) described malware as malicious software and one of the gravest hazards to computers and other electronic devices, such as phones and tablets. Malware can also infect databases (Harrington, 2021). Malware comes in many forms, including viruses, worms, rootkits, botnets, Trojan horses, spyware, and ransomware. These are dangerous programs that infiltrate a computer without the owners' or users' awareness and seriously endanger the users. Malware software typically has a genuine and safe appearance, but when it is downloaded, it corrupts and destroys computer systems, especially those that contain important data. "Rabbit" and "Bacterium," according to Lewis, Kaufman, and Christakis (2008), are two instances of malicious software that can wipe out a victim's PC.

The implication of using malware by cybercriminals to access the victim's computer systems and mobile devices is that they can access sensitive information and login details of the victims and use the same to scam them. This problem may be worsened by the likelihood that many Nigerians may be unaware of how to detect the presence of malware in their mobile devices or computers, while others may be unaware of practices by electronic device attackers or users (such as clicking on malicious links, opening unsafe messages, downloading malicious apps, etc.) that may introduce malware into their devices. Victims may equally experience malfunctioning devices resulting from malware attacks, which adversely affect the use of the infected devices in performing legitimate tasks.

Cyber identity theft/phishing

Identity theft is the illegal act of a person assuming the identity of another person in order to get sensitive personal data about that person. It is the assumption of another person's identity, whether they are alive or deceased, regardless of the reason for the behavior (Fafinski, 2008). Perpetrators of identity theft can be employed in the commission of drug, gun, and cybercrime-related offenses. It includes using a false identity to get goods, services, money, or other benefits (Australian Centre for Policing Research [ACPR], 2006). This is akin to the term "phishing," which refers to the practice of deceiving internet users by sending them bogus emails or webpages that appear genuine in an attempt to get personal data that can be used to commit identity theft. Phishing is analogous to the act of catching fish in bodies of water by fishermen using lures. In this case, the email being sent to potential victims represents the lure, the fish is the intended victim, and the criminal is the fisherman, while the offender makes use of the stolen data to their advantage. Identity theft is committed by an individual who obtains personal data from others and exploits it for their own gain. This can include a cybercriminal obtaining the login credentials and password to an individual's online bank account or an Automated Teller Machine (ATM) user's personal information and exploiting it to obtain large sums of money.

According to the Federal Bureau of Investigation [FBI] (2011), internet thieves make use of concealed recording devices to film people using the point of sale (POS) or ATM posts where withdrawals are performed without their knowledge. When the fraudsters play the recorded videos, they can obtain ATM card PINs and numbers entered into the machines by the owners while making transactions. As a result, when transactions are done through ATMs, a technique known as ATM skimming is used, which entails installing an electronic device on the machine to collect

data from the user's bank card's magnetic strip. Thereafter, the fraudster makes an attempt to criminally transfer funds from the bank account of the victim.

A person might also fall victim to online charity phishing, in which con artists create websites purporting to be charitable organizations and ask for materials and money donations to these fictitious organizations. Additionally, scammers run bogus social media profiles for charities with the sole purpose of obtaining donations from gullible people. Occasionally, they assert that certain people are in pitiable condition and are consequently in dire need of financial assistance to be rescued from life-threatening challenges such as homelessness, illness, and hunger, among others. They even go so far as to post images of the victim on phony websites that prove their illness. With this scheme, the scammers defraud the financial donors and enrich themselves. Another ploy used by fraudsters involves sending emails or SMS to people, telling them they have emerged as winners of online lotteries or lottery tickets. According to Rahman (2012), fraudulent cashier's checks have been used to deceive consumers by offering products for sale online or promoting items that are damaged or nonexistent and then requesting that the victims deposit a certain amount into an account or call a specific number.

Website Jacking/Cloning

Website cloning is the technique of creating a counterfeit website, whereas website jacking is the process by which hackers hijack or obtain access to and control over another website. In Nigeria, the development of phony websites that look authentic but are actually directed towards people who are unaware of the real company's website is also becoming more widespread. Here, internet users are tricked into thinking that a specific website is the one they really want to visit. But when consumers use their credit card information to order or make purchases on the scammers' website, their information is stolen. The criminals subsequently use the obtained data to trick the victim or sell it to other people who also want to use it to defraud the victims. The data stored on a certain website is altered or mutilated by the hijacker when it occurs (Abiola, 2019). These acts are carried out deliberately in order to achieve a variety of goals, as intended by the perpetrator. Unlike website hijacking, which is uncommon in Nigeria, website cloning is a prevalent practice. A number of times, the Department of State Services (DSS) has alerted Nigerians to the actions of certain fraudulent people who impersonate official government websites in an effort to defraud unsuspecting Nigerians (Sahara Reporters, 2019). Internet scammers employ website cloning to trick vulnerable individuals by using the legitimate identities of certain government

establishments. Ijeh (2019) claims that scammers have utilized ruses to trick both the Nigeria Social Investment Trust Fund (NSITF) and the National Youth Service Corps (NYSC) into believing their ploys.

Cloning of websites portends danger to the original website owners. The cybercriminals could use the fake website to initiate transactions and deals in the name of the organization whose website has been cloned. Cloned websites mislead the general public. The fake website could also be used to divert the clients of the victims, resulting in the low patronage arising from the loss of clients. Public trust and confidence in an organization could be lost if they get to know that the organization's website has been cloned. Consequently, the reputation of the organization would get damaged.

Software piracy

The stealing of someone's intellectual property is called piracy. Software piracy is the illegal copying, adjustment, duplication, and circulation of legally protected software such as films, games, music, etc. (Longe et al., 2008). There are now a lot more ways than ever to manufacture, store, replicate, distribute, and transmit stolen works because of new technology advancements. We might therefore conclude that having access to technology has aided piracy. Pirates buy original products, movies, or video games on the Internet and then illegally publish copies of them online for the public to access and use without the copyright owner's knowledge. To protect copyrighted materials, the Nigerian Copyright Decree No. 61 of 1970 was made (Ekwuazi and Mgbejume (2001)). In the same vein, Decree No. 47 of 1988 was made to protect the rights of authors (Ekpo 1992: 40). Similarly, Ekwuazi and Nasidi (1992) pointed out that the Copyright Act, Cap 68, Law of the Federation of Nigeria, as amended by Decree 98 of 1992 and Decree 42 of 1999, respectively, offers ample provision for the protection of the film producers. Despite the promulgation of these decrees, piracy persists in Nigeria. Software piracy has implications for the victim and the government. On the part of the victim, loss of revenue is one of the major implications of falling victim to this type of cybercrime because the revenue that should have accrued to the copyright owner gets diverted to the cybercriminal. The government, on the other hand, loses the revenue that could have been paid to it in the form of tax by the copyright owner if the intellectual property was not pirated.

Conclusion

The thriving of internet fraud in Nigeria indicates that the patterns of criminal victimization adopted by internet fraudsters produce the desired result for them. Internet fraudsters are clever, rational criminals that persist in using devious victimization patterns that allow them to outwit their targeted victims and reduce the likelihood of being apprehended and prosecuted.

Recommendations

The paper recommends as follows:

1. Regular enlightenment programmes should be used to educate the general public on the schemes adopted by internet criminals to defraud them.
2. Banks and other institutions should invest more in cyber security to prevent hacking into their systems and websites.
3. Security agencies should train more experts in the detection of cybercrime and provide them with the required technological tools to work with.
4. The punishment for arrested cybercriminals should be such that it counterbalances the criminal gain.

References

Abiodun, B. (2023). Hackers steal ₦2.9 billion from Flutterwave accounts, motion granted to freeze accounts connected with stolen funds. *Techpoint Africa*. Retrieved from https://techpoint.africa/2023/03/05/hackers-have-stolen-2-9-billion-from-flutterwave/ on 30/12/23

Abiola, A. (2019). What Nigerians lose yearly to cybercrime. *The Hope Newspaper.* Retrieved from https://www.thehopenewspaper.com/whatnigerians-lose-yearly-to-cybercrime/ on 19/12/2023.

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. Doi: 10.1089/cyber.2010.0307.

Aker, R.L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *Journal of Criminal Law and Criminology,* 81(3), 653-676

Business Day (2023). How to prevent mobile fraud. Retrieved from https://businessday.ng/big-read/article/how-to-prevent-mobile-fraud/#:~:text=How%20does%20mobile%20fraud%20happen,and%20apps%20from%20online%20platforms on 29/12/2023.

Coony, M. (2012). *10 common mobile security problems to attack.* Retrieved from https://www.pcworld.com/article/2010278/10-common-mobile-securityproblems-to-attack.html on 18/11/2021.

Dening, D. (2001) "Activism, and Cyber terrorism: The Internet as a tool for influencing Foreign

Policy," in John Arquilla and David Ronfeldt, ed.,Networks and Net wars. p. 241

Ejike, E. (2023). Fraudsters hack BVN, phone number to create multiple pseudo accounts. *Leadership*. Retrieved from https://leadership.ng/fraudsters-hack-bvn-phone-number-to-create-multiple-pseudo-accounts/ on 29/12/23

Ekpo, M. 1992, 'Towards a film policy for Nigeria'. In Ekwuazi, H & Nasidi,Y (Eds.) Operative principles of the film industry: Towards a film policy for Nigeria'. Jos: N.F.C.

Ekwuazi, H., Sokomba, J, Mgbejume, O (2001). *Making the transition from video to celluloid*. Jos: N.F.I

Ekwuazi, H., Nasidi,Y. (1992), "*No not nollywood : Essays and speeches by Brendan Shehu"*. Jos: NFI.

Fafinski, S. (2008). *UK cybercrime report. Retrieved from* http://www.garlik.com on 01/01/2023

Federal Trade Commission (2021). How to recognize, remove, and avoid malware. Retrieved from https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware on 29/12/23.

George, G. (2023). Bank customers, companies lose billions to Nigeria's weak cybersecurity. Punch. Retrieved from https://punchng.com/bank-customers-companies-lose-billions-to-nigerias-weak-cybersecurity/

Hall, G., & Watson, E. (2016). Computer hacking, security testing, penetration testing, and basic security. Retrieved from http://repo.darmajaya.ac.id/3932/1/Hacking.%20%20Computer%20Hacking%2C%20Security%20Testing%2CPenetration%20Testing%2C%20and%20Basic%20Security%20%28%20PDFDrive%20%29.pdf on 30/12/23

Harrington, J.L. (2021). Database security. Retrieved from https://www.sciencedirect.com/topics/computer-science/malware on 29/12/2023.

Harvy, C. (2017). Types of malware and how to defend against them. *Security Planet.* Retrieved from https://www.esecurityplanet.com/malware/malwaretypes.html on 13/11/2023.

Idris, A. (2020). Two Nigerian banks have been hacked, they deny it, here's a bigger problem. Retrieved from https://techcabal.com/2020/09/01/two-nigerian-banks-have-been-hacked-they-deny-it-heres-a-bigger-problem/

Ijeh, M. (2019). DSS raises the alarm! Nigeria government's official website is being cloned. Retrieved from https://metrowatchonline.com/dss-raises-the alarm-nigeria-governments-official-website-is-being-cloned/ on 16/2/2023.

Makeri, Y.A. (2017). Cyber security issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), 315-321

Okeh, A. (2023). Fraudsters hack 1000 accounts using BVN linked numbers. *Punch*. Retrieved from https://punchng.com/fraudsters-hack-1000-accounts-using-bvn-linked-numbers/

Police Special Fraud Unit (2021). SFU arrest bank hacker over ₦1.87 billion fraud. Retrieved from https://www.specialfraudunit.org.ng/en/?p=1186 on 30/12/23

Sahara Reporters (2019). Scam: DSS raises the alarm over cloning of government official websites. Retrieved from https://saharareporters.com/2019/07/19/scam-dss-raises-alarm-over-cloning-government-official-websites

Siegel, L. (2005). *Criminology: The core*. Belmont: Thomson Wadsworth

Symantec (2016). Cyber crime & cyber security trends in Africa. global forum for cyber expertise (gfce) initiative. Retrieved from https://www.cybercrime and cyber security trends in Africa. 18/12/2023.

The Economic Times (2023). What is "hacking"? Retrieved from https://economictimes.indiatimes.com/definition/hacking on 29/12/23

Waters, P. (2021). Time to compromise: How cyber criminals use ads to compromise devices through piracy websites and apps. Retrieved https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4536943 on 29/12/2023

Urbas, G. & Choo, K.R. (2008). *Resource materials on technology-enabled crime, AIC, Canberra.* p.83; AIC, High tech crime brief: Hacking offences, AIC, 2005, p.1.