Chapter 4
Social Media and Cyber Security:
Investigating the Risk in Nigeria

Desmond Onyemechi Okocha
https://orcid.org/0000-0001-5070-280X
Bingham University, Nigeria

Damilare J. Agbele
Bingham University, Nigeria

ABSTRACT

The proliferation of social media in Nigeria has birthed new paradigms of communication and two-way interactions among friends, family colleagues, and business associates. It has equally morphed to become a channel for money generation among enterprising youth across the nation. It cannot be denied that the merits associated with this phenomenon called social media are enviable; however, it is also arguable that cyber security is a key factor to the enjoyment of these attendant benefits. This study is anchored on the protection motivation theory and the technological determinism theory. The study identified some cyber security risks synonymous to the use of social media in Nigeria. To remedy the situation, the study recommends that education and practical training in technological best practices in formal and non-formal school settings will help mitigate the inherent risks discussed. Also, initiatives should be taken by the government and organisations to curb this serious issue.

INTRODUCTION

Social media is one out of the platforms provided by the evolution of new media technologies. It is perhaps the most popular and people identify with it owing to its capacity to generate user-defined contents, facilitate two-way communication without the problem of time and boundaries. Social media encompasses all platforms founded of the web 2.0 technology – the technology that expedites the generation and exchange of contents (texts, images, videos, and sounds) by users. It is affirmed that social media hinges on either mobile or web-based technologies to create conversational network/groups where

DOI: 10.4018/978-1-7998-8641-9.ch004

individuals and communities share, comment, discuss and modify user-generated contents (Toivo-Think Tank, 2012) classified social media into six categories, they are:

- Social Networks, e.g., Facebook, Google+, Myspace, and LinkedIn
- Media Products Community/Content sharing, e.g., YouTube, Flickr, and SlideShare
- Blog Services, e.g., Wordpress, Blogger, and Twitter
- Information Community/Collaborative communities, e.g., Wikipedia and Wikispaces
- Virtual Communities. These are also called Virtual Game Worlds
- Link Sharing Services, e.g., Digg and Diigo

Social media exists in the form of smartphone applications and websites and some of the most utilized in Nigeria are Facebook, WhatsApp, Instagram, and Telegram. Asides from the ease of communication made possible by the social media, it has also evolved to become marketing channel whereon enterprising Nigerian youths advertise/market their products and services. Thus, the medium is a communication cum marketing platform.

The statistics (2021) estimates that as of January 2021, Nigeria has estimated 33 million social media users. This explains the large number of people who visit social media platforms to link-up with friends and to sustain connections, be it professional or personal reasons. Scholars have argued that as much as social media platforms have provided many opportunities for transformation and advancement of humanity in the society through interactive information exchange, it has also created catalogue of challenges that the society is presently contending with (Agbawe, 2018). Popular among these challenges is the issue of cyber threat, i.e., threats to the safety and security of social media users. These threats can be direct or indirect and they take different forms. Some of the common ones are account cloning, access to private information, hacking, phishing among other things. Social media companies, organizations and individual users are becoming more concerned about how to reduce the risk of unauthorized access and loss of their private information, hence more attention to cyber-security. This discussion will examine social media and its penetration in Nigeria and the cyber breaches common to social media. Two landmark cases of cybercrimes in Nigeria in recent years will be examined, as well as strategies to mitigate against cyber security breaches in a developing nation like Nigeria.

RESEARCH OBJECTIVES

The underlining aim of the study is to improve the available body of research works related to social media and cyber security in Nigeria. The driving specific objectives are:

1. To review the history of social media in Nigeria
2. To examine cyber breaches common to social media in Nigeria
3. To identify strategies to mitigate against cyber security breaches in Nigeria

RESEARCH METHODOLOGY

This study adopted the qualitative desk research approach. It critically reviewed secondary data from academic papers and published print materials (online and hardcopy) that are peculiar to the discourse. Eight cases of cyber-related crimes committed by Nigerians were profiled in the study.

Theoretical Framework

This study is hinged on Protection Motivation Theory (PMT) and Communication Privacy Management Theory (CPMT). The protection motivation theory (Rogers, 1975) explains that the intention of an individual to protect him or herself depends on four perceptions, these are; the severity of a threatening situation, the probability of occurrence, the efficacy of the commended preventive behavior by the individual, and the individual's self-efficacy. Social media platforms have tendencies of exposing users to a variety of online security threats that requires them to activate safety mode. PMT predicts the utilization of protective technologies which help users escape harm from negative technologies by practicing healthier behaviors when dealing with issues that are security-related (Boss, Galletta, Lowry, Moody, & Polak, 2015). This study adopts PMT because it helps to understand behaviors that guarantee safety in the context of social media use.

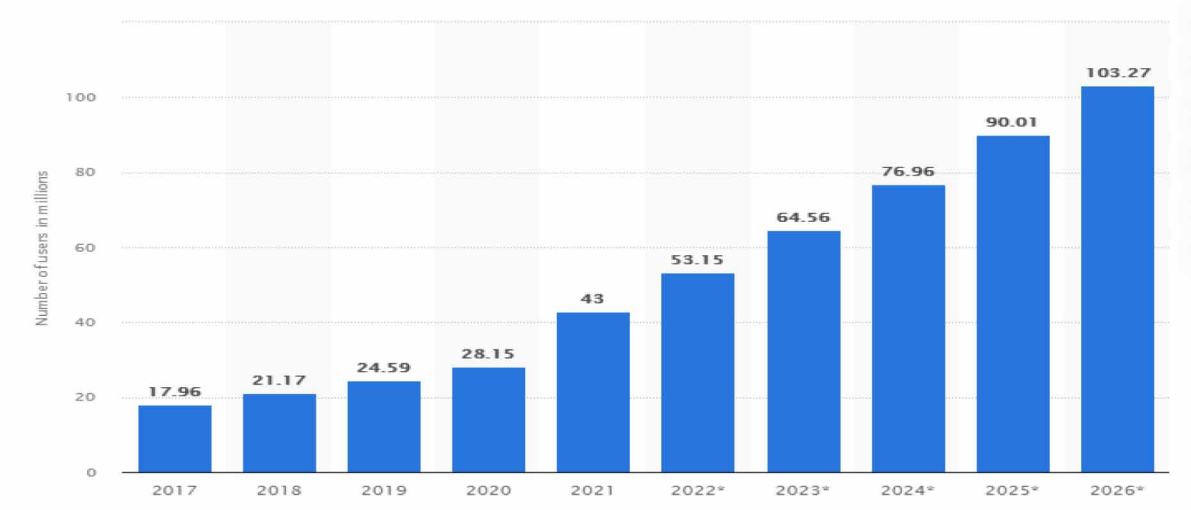
Communication Privacy Management Theory was developed by Sandra Petronio in 1991, it explains the believe that people have ownership rights to their private information but somehow miss the part that when they disclose any information to others, they have made themselves vulnerable in a way or another. Petronio (2004) explains the need for controlling private information. Petronio notes that once private information is shared with others, ownership of such information is not secured anymore, and one can't decide what happens to the information after such information has been shared on social media. Social media users interact with each other and share private and public information. The theory encourages social media users to build privacy boundaries by knowing whom they disclose their private information to. This study adopts the communication privacy theory because it helps social media users understand the importance of information privacy when setting up and/or using social media platforms, and to be conscious of building privacy boundaries to avoid issues of vulnerability.

SOCIAL MEDIA IN NIGERIA: HISTORY, PENETRATION AND USAGE

Social media adoption in Nigeria can be attributed to the growth of Information Communication Technologies (ICTs) which began in the 1990s. Golub (2018) notes that the very first technological evolution seed sown into the Nigerian soil was in 1995 when UNESCO-sponsored the Regional Informatics Networks for Africa (RINAF) project. The project had the objectives of ensuring that new information and telecommunication technologies favour exchanges between African countries; remedy the isolation of development and research institutions in African countries and facilitate dialogue between researchers, academics, and industrialists; develop an operative process for the coordination, integration and upgrading of African networks, as well as exchange with other international networks. In the same year, the Nigeria Internet Group (NIG) was formed as a non-governmental organization, and the group held workshops around the country to increase the level of awareness on benefits of Internet for Nigeria. In 1996, internet officially penetrated Nigeria after the Nigerian Communications Commission (NCC) agreed

to issue license to internet service providers. Linkserve Ltd. was the first licensed Internet provider and it started operations on January 1, 1997. Between the year 1996 to 2000, more internet service providers gained licenses from the NCC, these brought about greater access to the internet as more internet exchange points were built around the country.

Figure 1. Rate of Internet Penetration in Nigeria



Nigeria opened up its borders for ICTs and eventually came up with information technology policy to improve the use of technology for development in the late 1990s and the beginning of the millennium (Igyuve and Agbele, 2016). This development allowed ICT and its ancillary technologies to gain footings in Nigeria as people were able to communicate virtually from computer systems and the internet-enabled phones, starting with emails. The internet user figure in Nigeria stands at 104.4M as at January 2021 (Kemp, 2021), Statistica (2021) notes that there an estimated 33 million social media users in Nigeria as of January 2021 and projects that the figures will hit 43M by the end of the year (See chart). This statistic explains how social media continues to permeate the lives of Nigerians. At present, it seems that one could hardly find a place in Nigeria, where people do not use social media.

After year 2000, more user-friendly social networking sites sprang up and become known in Nigeria, the likes of Myspace, Facebook, 2go are examples. This greatly enhanced two-way and instant communication between/among people and groups who share common interest. Today we have more conventional social media platforms that Nigerians are registered in which they engage to communicate, transact, and socialize. Some of these platforms are Wikipedia, Friendster, LinkedIn, Hi5, Instagram, WhatsApp, Tik-Tok, Triller, Snapchat, and Telegram. Other social media platforms were purely Nigerian-oriented, hence, they catered specifically for the need of Nigerians, some of these are NaijaPals and NairaLand (Uwem, Enobong, and Nsikan, 2013).

A Pew Research Centre survey in March 2021 revealed that social media engagement has a correlation with having network of diverse friends and connections, especially in economies that are emerging. This exposition explains the primary utility of the social media which is to allow people keep in touch with family and friends. The use also attempts to do more formal forms of communication such as business

discussions and networking. People also use social media platforms to source for career opportunities, connect people with like interests across the globe, and share insights. Asides from the basic communication, social media is also engaged for marketing purposes, building brands & online presence and disseminate new stories. Akanni (2012) also discovered that social media serve as a tool for socialization, enhances learning opportunities, communication, entertainment, political participation, and instant messaging as the uses of social network sites among Nigerians.

CYBERCRIME: CASES IN NIGERIA

Cybercrime entails the use of computers, network device(s) or a network to further illegal/fraudulent course. In Nigeria, cases of cybercrimes are no longer new. Cases of arrest of cybercriminals are becoming quite popular in the media too. Two popular cases are profiled below.

On the other hand, the US Department of Justice divided cybercrime into three categories (Brush, 2020). These categories are;

- Crimes where computer gadget is the target (to gain illegal access).
- Crime wherein the computer gadget is used as a weapon (using the computer for credit card fraud or cyber terrorism).
- Crime in which the computer is used as an accessory to crimes (e.g., storage of illegal document).

The necessity of internet connectivity and heavy social media presence has enabled and increased the volume and pace of cybercrime in recent years. Cybercrimes can be planned and executed by an individual or a group and the aim is to exploit the vulnerability of social media users.

The Hushpuppi Case and Others

News broke on June 20, 2020, that popular Nigerian and social media influencer popularly known as Ray Hushpuppi had been arrested in Dubai where he lived. Until his arrest, he lived a luxurious life and had followership of about 2.5M on Instagram. Hushpuppi (38yrs) usually posts videos of himself playing with wads of cash and flaunting wealth but had always maintained that he was a real estate developer. CNN reported that a Federal affidavit alleged Hushpuppi's extravagant lifestyle was financed through hacking schemes. The affidavit further alleged that Hushpuppi stole millions of dollars from companies in USA and Europe. His flamboyant posts on the internet left digital trails of evidence that investigators used to link him to the cybercrimes. Hushpuppi was arrested in Dubai and was extradited to the United State to face trail for conspiring to launder millions of dollars through cybercrime. Hushpuppi is alleged to lead a global network of cyber criminals that use business email compromise, money laundry, and computer intrusions strategies to steal from individual and companies. Hushpuppi was arrested along with 11 cohorts and investigators were reported to have seized items worth 41 million US Dollars, 13 luxury cars worth 6.8 million US Dollars, smartphones and computer evidence, Dubai Police said in a statement. Email addresses of nearly 2 million possible victims on phones were uncovered, computers, and hard drives. (Source: CNN News, 2021). The trial is currently on in the USA soil and Hushpuppi has pleaded guilty to his crimes.

Another case was published by the Interpol in November 2019 when the InterPol declared the arrest of three Nigerians in Lagos for cybercrime investigation. The suspects were arrested following a joint taskforce operation by the Group-IB, INTERPOL and Nigeria Police Force following a year-long investigation with the code-named 'Operation Falcon'. The three Nigerians are believed to be members of a wider organized crime group – a group responsible for carrying out phishing campaigns, distributing malware and extensive business email compromise scams. It was alleged that the suspects developed phishing links, domains, and mass mailing campaigns through which they impersonated representatives of different organizations. Through this fraudulent mailing campaigns, 26 malware programmes were disseminated through spyware and remote access tools. These programmes were used to penetrate exiting cyber securities and monitor the systems of individuals and victim organizations. Afterwards, scams were launched, and funds were syphoned. The gang is believed to have compromised government establishments and private sector companies in more than 150 countries since 2017 (Source, The Interpol).

The security agency in charge with investigating related cybercrimes in Nigeria is the Economic and Financial Crimes commission and the Lagos zonal headquarter of the Agency reported that they have arrested 44 suspected internet fraudsters in Lagos, during different operations in some parts of Lagos State between June 1, 2021, and June 3 (The National News, 2021). The BBC in February 2021 also reported the 10 years sentence judgement of 33yearsd old Nigerian, Okeke Obi (also known as Invictus Obi) by the East Virginia District Judiciary. Okeke Obi was sentenced after being found guilty of cyber fraud that has led to the theft of about 11million US Dollars (equivalent to 8 million British Pounds). Obi primarily used Nigerian-based companies to defraud people in the US. According to the report, Obi was part of a group which engaged in cybercrimes between the years 2015 to 2019. Obi was also accused of working with conspirators to create profiles of hundreds of victims including people in the US's Eastern District of Virginia. In one phishing attack in 2018, Obi and his gang gained access to the email of a manager at Unatrac Holding Limited, the export sales office for Caterpillar's heavy industrial and farm equipment. Thereafter, fraudulent wire transfers to the tune of nearly $11m was made and the funds was moved overseas.

In November 2019, the US Department of justice charged ten Nigerians in the US with conspiracy to launder proceeds that were fraudulently obtained from Nigerian romance scam operation targeting multiple victims. The indictment alleged that since 2017, the co-conspirators coordinated with unknown individuals in Nigeria who assumed false identities on online dating sites and social networking sites to defraud unsuspecting victims. The individual told the victims they were U.S. residents working abroad and thereafter, romantic relationships were formed. At the early stage, victims would receive requests of gift cards and cell phones. As the relationships continued, the requests would develop into increasingly larger sums of money intended to complete projects or to return to the United States.

The victims were directed by the online romance scammers to send funds to the defendants' bank accounts. The defendants concealed the proceeds of romance scam operations by moving money between and among multiple bank accounts that were opened using fraudulent identity documents to obscure the source of the funds and the identities of the co-conspirators. They also purchased salvaged vehicles and car parts to export overseas, usually to Nigeria, to conceal the sources. As published on the US department of justice website, their names are Afeez Olajide Adebara, (34 years) U.S. citizen; Oluwaseun John Ogundele, (30 years) U.S. citizen US; Joshua Nnandom ditep, (25 years) Nigerian citizen; Paul Usoro, (25 years) Nigerian citizen; Chibuzo Godwin Obiefuna Jr, (26 years) U.S. citizen; Jamiu Ibukun Adedeji, (23 years) Nigerian, residing in Norman, Oklahoma; Tobiloba Kehinde, (27 years) Nigerians.

The last three names were unknown as they were still at large as at press time, but they were confirmed to also be residing in the US as at the period of the crimes, just like the first seven.

Another 52 internet fraudsters were arrested by operatives of the Benin Zonal Office of the Economic and Financial Crimes Commission (EFCC) on May 11, 2021 (Premium Times, 2021). The anti-graft Agency indicated that the suspects were involved in romance scam on social media, using fake identities of Caucasian men or women to defraud unsuspecting victims of their hard-earned monies. Items recovered from the suspects at the time of arrest include fake identity cards, six exotic cars, laptop, mobile phones, and documents.

Similarly, two Nigerian youths were convicted of cybercrimes and sentenced to two years imprisonment by the Edo State High Court in Benin City, Edo State. on July 19, 2021 (Channels TV, 2021). The defendants, known with the monikers Frank Mark (real name being Noah Omoregbe) and William Scot (real name being Destiny Efewengbe) were arraigned on one count charge each of impersonation and fraudulent intentions, contrary to section 484 of the Criminal Code Law Cap 48 Laws of defunct Bendel State of Nigeria (as applicable in Edo State) 1976.

The Federal High Court in Port Harcourt, Rivers State also convicted and sentenced two Internet fraudsters, Jonathan Collins and Godspower Ofonime, to six years imprisonment each for internet fraud after being arraigned by the EFCC. One of the charges against Collins stated that Jonathan Collins (Alias Janis Louise Hughes; Allan Carmack Calluk; Dr. James Lattimore) fraudulently impersonated one Janis Louise Hughes, a white man from Glenville, North Carolina, USA with the intent to obtain money from unsuspecting men and women. (Francis and Naku, 2021). Ofonime met his waterloo when verified intelligence by the EFCC linked him with scam emails to foreigners.

Popular Nigerian newspaper, Daily Post also reported the arrest and conviction of two Nigerians internet fraudsters (Tolani Bakare and Alimi Sikiru) by the Lagos State High Court following a suit by the Economic and Financial Crimes Commission (EFCC) in August 2021. Bakare, claimed his forte is business email compromise and confessed to have hacked into different companies outside the shores of Nigeria and the accounts of KLM Airline, Turkish Airline and British Airways. The second defendant, Sikiru, in his statement to the EFCC, admitted that majority of the funds found in his account were from the first defendant, Bakare. The convicts forfeited over N200 million and properties in the upscale Lekki axis of Lagos to the Federal Government. These cases explain the rate at which cybercrimes continue to increase in Nigeria, hence the need to seek ways to address the situation.

SCHEMES UTILIZED BY CYBERCRIMINALS

Cybercriminals can be described as people who engage in criminal activity by using computers and internet (Oxford Dictionary, 2021). Some of the schemes employed by cybercriminals are:

- **Cyberstalking:** This is the use of the internet connectivity and other computer-based technologies to harass or stalk other persons in the online space (Gordon, 2021). Cyberstalking has a fixated pattern and obsessions behaviour by the cybercriminals, it is intrusive, causes fear and endangers alarm in victims. The Cyber Helpline (2020) list some of the common stalking activities of cyber stalkers to include; unsolicited messages, information gathering, surveillance, unauthorized access to online accounts and spread of misinformation. Victims of cyberstalking are usually known

persons to the cyber stalker. Cyber stalkers could be an ex-lover, colleague or known crush. In some cases, the cyberstalker could be an unknown person totally.

- **Phishing Attack:** This is a kind of cybercrime where a malicious link or attachment file is sent by the intruder to harvest personal information from the victim's system, once clicked on - information such as username and password, credit card information, online banking information. Baykara and Gurel (2018) also mentioned that people who commit this crime often gather background information from social media platforms and other public information resources such as Twitter LinkedIn or Facebook about victim's personal work history interests and activity. When the study is completed friend requests are sent to the victim or they are followed online sometimes the links or messages just come out of the blue.
- **Cyberbullying:** Adeniran (2020) & Balogun et al (2017) observed that's cyberbullying is becoming a common phenomenon in Nigeria and that it is rampant on social media platforms where a lot of people are subscribed. Cyber bullying is that trolling, catfishing, blatant harassment, and mistreatment of people online (Iyanda, 2020). Cyber bullying is the utilization of smartphones or social media platforms to embarrass other persons. It is carried out in various ways, one of which is posting the naked picture of someone online, projecting a part or type of body of someone on the social media for the purpose of embarrassment (popularly called body shaming), revealing personal information about someone without their consent (also called doxing), this could be photos, documents, phone numbers, and addresses.
- **Cross-Site Scripting (XSS):** Cross-site scripting is one of the most common forms of attack on web-based applications (Almarabeh & Suleiman, 2019). In cross site scripting, harmful codes are inserted into sites or applications to be opened in system browser. The intention is to remotely steal cookies (that is text files with small pieces of information, e.g., username and passwords), modify the websites, capture clip boards contents, scan ports and download (Raman, 2008). This also leads to account hacking.
- **Clickjacking:** This is an attack that tricks social media users to click on hidden elements such as unintended links so they would end up on malicious websites or download viruses and disruptive software. As mentioned by Lundeen and Rhodes (2011), cybercriminals can use the hardware of user computers such as camera and microphone to record their activities.
- **Account Cloning:** This is it a technique used by cybercriminals to create a fake profile by using personal information, images and/or video stolen from the profile of targeted social media users (Almarabeh, 2015). This can be done manually or automatically (through written programme codes). In most cases, accounts that are cloned are usually set as public, so all information of the user are available to everyone, including the cybercriminal. Through cloned accounts, cybercriminals send messages to targeted audience most times for money extortion.
- **Harvesting of Private Information:** Cybercriminals can also set out to harvest private information of social media users to harm them. Social media users who are more susceptible to it are those who usually reveal their health status, show-off their wealth in the social media space, reviewed all their locations publicly, bank details and information that are sensitive. Leakage of this sensitive information could hold negative implications for social media users. Maremot (2010) cited an example of insurance companies who now use social media data to distinguish between risky and safe clients.
- **Romance Scam:** This is one of oldest cybercrime approach known in Nigeria. It is a situation where cyber criminals create fake profiles on social media with the intention of swindling lovers.

Cyber criminals in this case play on emotional triggers to get partners to provide them with money gifts or personal information.

CYBERCRIMES IN NIGERIA: CAUSES AND EFFECTS

Statistics shows that a significant proportion of cybercrimes are perpetuated by youths (Ibrahim, 2019). Cybercrime can be attributed to factors such as high youth unemployment, negative role-modeling, desire for wealth, weak implementation of cyber laws, poor education of internet users on cybercrimes, corruption, the vulnerable nature of the internet and the laissez faire attitude of individuals and businesses regarding cyber security (Hassan, Lass & Makinde, 2012).

Causes of Cyber-Crimes in Nigeria are discussed below.

- **Unemployment and Poverty:** This is perhaps the major causes of cybercrime in Nigeria. Unemployment rate in Nigeria stood at 33%, as at the last quarter of 2020 (Olurounbi. 2021). High rate of unemployment has consequential effects, some of which are socioeconomic, political, and psychological consequences. The issue of unemployment automatically increased the rate at which people take part in criminal activities for their survival. Unemployment encourages the development of cybercrime among youths who constitutes a large percentage of the unemployed workforce. There is a connection between unemployment and poverty as one who is not gainfully employed will most likely be poor. The 2019/2020 Nigerian living standards survey released by the National Bureau of Statistics, NBS, shows that 82.9 million (40.1 per cent of the population) Nigerians are poor. A poverty-stricken person may very liable turn to crime for survival.
- **The 'Quest for Wealth' Culture:** The culture of hard work, honesty and integrity are fast failing in the Nigerian society. Nowadays, youths tend to be greedy and are not ready to start small; they strive to level up with their rich counterparts by engaging in cybercrimes (Ibrahim, 2019 and Omodunbi, Odiase, Olaniyan & Esan, 2016).
- **Negative Role Modeling and Corruption:** Meke (2012) notes that parents transmit criminal tendencies to their children through the process of socialization. This means that some children pick up criminal tendencies from their parents. Additionally, Nigeria, at the end of the year 2020 ranked 149 on the global ranking of corrupt countries after surveys by the Transparency International (Vanguard Newspaper, 2021). The Nigerian society also celebrates wealth without care or question on the source of such wealth. This misguided disposition encourages the get-rich-quick mindset that can be fed through cybercrimes as younger ones tend to model their lives after celebrated 'criminals' in the society.

Brush (2018) adduced that the true cost of cybercrime is difficult to assess accurately. This implication of this statement is that the effect of cybercrimes on the society cannot truly quantify as it cuts across different spheres of the nation and indeed the social media users. Starting with the social media user, users who are online victims of cyber-attacks suffer from emotional trauma, which could lead to depression and acute stress disorder (Lynn, 2007). In most psychological cases, victims of cyber-attack feel they are to be blamed for the attack because they let their guards down, they therefore prefer not to involve anyone, live in isolation, and not even report the case.

- **Ill-equipped Law Enforcement Agencies and Implementation of Cybercrime Laws:** African countries have received constant criticism for inadequately handling the implementation of policies. This appears the same for Nigerian Cybercrimes (Prohibition and Prevention) Act, 2015. The Act makes provision for the protection of people, property, and the government against unethical internet practices (Uba and Agbakoba, 2021). However, it saddens that Nigeria continues to experience great effects of cybercrime. Internet fraud appears to be everyday job of some Nigerians owing to weak implementation by agencies managing the Act's implementation. These agencies are trying but in some ways some perpetrators get off the hook when apprehended. This in a way encourages offenders to commit more crime, knowing that they can always escape the wrath of the law.

Asides from the above listed, cybercrimes in Nigeria can also be attributed to poor education of social media users on the issue. A good number of social media users don't read terms and conditions, especially with regards to privacy when registering on social media sites. Kumar et al (2013) observed that some social media users put themselves at risk of cybercriminals too as the amount of personal information they leave as public on their social media platforms can give them away. People also tend to read less about new methods used by cybercriminals and what to do to avoid them, as disseminated by the mass media. The relaxed attitude of individuals and businesses towards online security is also a challenge. Aladenusi, a cyber risk expert attributed the rise in cyber frauds to insufficient skilled resources, deficiency in awareness, rapidly changing technology landscape and weakness in cyber security controls (All Africa News, 2021).

Ogunjobi (2020) also advanced other effects of cybercrime, some of which are huge cost required by organizations to fix damages caused by cybercriminals with a view to preventing a repeat of such. Other effects are reputational distrust, loss of creditworthiness for people whose have suffered identity theft. The kind of life that cybercrime provides, e.g., lavish lifestyle, flaunting of wealth on social media, clubbing, and other social pump gatherings have also reduced the love for true education and hard work among youths. Youths today go as far as withdrawing from school to join the pyramid of cybercriminals. A lot of youths who would have contributed meaningfully to the nation are now recruited, trained, and mentored by the godfathers in internet fraud.

Another major effect of cybercrime is revenue losses to nations and social media users. Allogo (2021) reported that Nigeria lost 5.5 trillion Naira to fraud and cybercrimes in the last 10 years. Cybercrimes disruption of business causes profit pilferage, and welfare losses. Cybercrime also have national security implications; therefore, manpower and funds are channeled to the government to avoid a collapse of the nation to external hackers. During the #EndSars protest in October 2020, popular hacking group called *'Anonymous'* claimed via its Twitter handle, that it had infiltrated some Nigerian government and business organisation websites (Adeshina, 2020) in support of the protest that took over many cities in Nigeria. This protest evolved following calls for the disbandment of the special police unit called the Federal Special Anti-Robbery Squad (FSARS). The group was reported to be involved in the abduction, harassment, extortion, and murder of innocent Nigerian victims. It was alleged that the 'Anonymous' group infiltrated a popular Telcom operator in Nigeria and gave 1000 NGN credit to all users. The Telecom Company came out to deny this breach.

CYBERSECURITY - MITIGATING AGAINST CYBER BREACHES IN NIGERIA

Cyber security is a practice of keeping computer systems, networks, and programmes safe from cyber-attacks. Eweniyi and Frank (2013) gave a scholarly definition of the term cyber security. To them, cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. As discussed earlier in this study, social media users, be its private persons or business organizations are susceptible to various forms of calculated cybercrimes therefore steps must be taken to ensure security. Cisco (2019) is of the opinion that cybersecurity approach that would be successful would have multiple layers of protection that spread across the computers networks programs or data that one intends to keep safe. This means that addressing cybercrime is not a one-way affair, it is a multilayered approach. There is a need to involve people, processes, and technology. This study believes that mitigation of cybercrime is a role of three, entities namely, the individuals (social media users), organisations (social media companies and other organizations and the government.

At the social media user level, Kumar et al (2013) advised users to protect themselves online by reducing personal information put online so that chances of cybercriminals piecing together one's routine becomes limited. Social media are expected to be comfortably safe about what they post online. If possible, users should google themselves and see if very personal information like address, phone number or places regularly visited is public. If this information are public, find a way to bring them down by contacting the site. Also, social media users should reduce the use of third-party applications that makes their way around the major applications like cameras and beautifying applications. Almarabeh & Suleiman (2019) gave some tips regarding social media safety in the wake of cybercrimes, they suggested that social media users take the advantages of all update notifications on the site and applications which are continuously developed to improve the level of data security. Users should carefully review any social media users' terms before accepting them. Many social media platforms use GPS tracking to tag user location to posts and photos, this can be turned off in the settings. Social media users who feel stalked should not hesitate to tell those around and report such to the right authorities. Self-security and privacy consciousness is important.

The government and organizations should also embark on cybercrime literacy campaigns. Tayouri (2015) believes proper training can raise necessary awareness and personal responsibility to help prevent social media cybercrimes. Organizations should also provide effective security trainings for staff on best practices in social media use, threats, precautions, policy and how to report when there is breach. On the part of organization, Organizations should beef up IT systems and protect critical information infrastructure. Chi (2011) suggested that organizations should ensure the internet security firewalls are up to date, that anti-virus and anti-spy software are installed on employees' systems and other devices they use. Finally, the Nigerian government should also strengthen her agencies so that more can be achieved in the fight against cybercrime. Cyber legislation can also be constantly reviewed so that new trends in cybercrime can be addressed as they evolve.

CONCLUSION

Social media has offered novel ways of interaction and communication, similarly it has brought about new security and privacy challenges. These challenges include cyberstalking, phishing attacks, cyber bullying, cross-site scripting, cyber jacking, account cloning, harvesting of private information and romance scam. Equally, the study revealed that cybercrime is a problem in Nigeria and various factors have sustained the challenge. The study mentioned some of these factors/challenges; they are poverty, unemployment, wrong modeling and societal values, desire for wealth pop culture, ill-equipped law enforcement agencies and implementation of cybercrime laws, poor education about cybercrimes, weak structures of organization internet systems. Cybercrimes effect also cut across the political, economic, social, technology domains of Nigeria. Large amounts of money is lost to cybercrimes every year while victims also suffer losses, even their lives sometimes. In order to reduce the risk of Cybercrimes in Nigeria in the social media, strategic measures should by every stakeholder in the social media industry, i.e., the social media users, the government, and the social media companies. The government should create jobs as the idle hand is the devil's workshop. An enabling environment for job creation by youths and entrepreneur will help to tackle unemployment and poverty considerably, thereby help reduce crime rates, especially cybercrime. Stringent laws that reduce the participation of youths in cybercrime should be enacted and enforced by the government of the day in Nigeria. Parental, families and the society should revert to the teaching of virtues such as integrity and hard work, this will help to produce better individuals in the society. Parent and people in positions of authority/influence should stand as good role model to Nigerian youths. There should be massive education on cybercrimes and how to avoid them by organizations, social media companies and the government, as this will help social media users.

REFERENCES

Adediran, A. (2020), Cyberbullying in Nigeria: Examining the Adequacy of Legal Responses. *International Journal for the Semiotics of Law - Revue internationale de Sémiotiquejuridique,* (34), 29.

Adeshina, O. (2020). *Popular Hacking Group "Anonymous" Allegedly Hacks Nigerian Government Websites*. https://nairametrics.com/2020/10/15/endsars-popular-hacking-group-anonymous-allegedly-hacks-nigerian-govt-websites/

Almarabeh, H., & Suleiman, A. (2015) The Impact of Cyber Threats on Social Networking Sites. *International Journal of Advanced Research in Computer Science, 10*(2).

Alogo, U. (2021). *West Africa: 'Nigeria Lost N5.5 Trillion to Cybercrimes in 10 Years*. Retrieved from https://allafrica.com/stories/202104260948.html

Ayakoroma, F. B. (2008). #Endsars: Popular Hacking Group, Anonymous Allegedly Hacks Nigerian Govt. Websites Reinventing the Pollical Process in Nigerian Video Films: A Critical Reading of Teco Benson's "The Senator". *Nigerian Theatre Journal.*, *14*(2), 1–21.

Balogun, N. A., Awodele, T. A., Bello, O. W., Oyekunle, R. A., & Balogun, U. O. (2017). Impact of Social Networks on the Increase of Cyberbully Among Nigerian University Students in Ilorin Metropolis. *Journal of Science and Technology*, *8*(2), 102–111.

BBC. (2021). *Obinwanne Okeke: Nigerian Email Fraudster Jailed for 10 Years in US*. Available at https://www.bbc.com/news/world-africa-56085217

Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The Impact of Polices in Government Social Media Usage; Issues, Challenges And Recommendations. *Government Information Quarterly*, *29*(1), 30–40. doi:10.1016/j.giq.2011.04.004

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). *What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors*. Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2607190 doi:10.25300/MISQ/2015/39.4.5

Chai, S., Bagchi-Sen, S., Rao, H. R., Upadhyaya, S.J., & Morrell, C. (2009). Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182. doi:10.1109/TPC.2009.2017985

Channels, T. V. (2021). *Court Sends Two Internet Fraudsters to Two Years in Prison*. Available at https://www.channelstv.com/2021/07/19/court-sends-two-internet-fraudsters-to-two-years-in-prison/

Chiemela, Q. A., Ovute, A. O., & Obochi, C. I. (2015). The Influence of the Social Media on the Nigerian Youths: Aba Residents Rxperience. *Journal of Research in Humanities and Social Science*, *3*(3), 12–20.

Cisco. (2019). *What is cybersecurity?* Available at https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-work

CNN. (2020). *He Flaunted Private Jets and Luxury Cars on Instagram. Feds Used His Posts to Link Him to Alleged Cybercrimes*. Available at https://edition.cnn.com/2020/07/12/us/ray-hushpuppi-alleged-money-laundering-trnd/index.html

Cyber Help Line. (2019). *Cyber Stalking*. https://www.thecyberhelpline.com/guides/cyber-stalking

Daily Post Newspaper. (2021). *Two Internet Fraudsters Convicted in Lagos, Forfeit Assets to FG*. Available at https://dailypost.ng/2021/08/09/two-internet-fraudsters-convicted-in-lagos-forfeit-assets-to-fg/

Francis, O., & Naku, D. (2021). *Man Bags Two-Year Jail Term For Currency Counterfeiting*. Available at https://punchng.com/two-internet-fraudsters-jailed-six-years-in-rivers/

Gaolub, K. (2018). *History of Social Media in Nigeria and the World*. https://www.legit.ng/1209780-history-social-media-nigeria-world.html

Gordon, S. (2021). *What Is Cyberstalking?* https://www.verywellmind.com/what-is-cyberstalking-5181466

Ibikunle, F. & Eweniyi, O (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education, 1*(1).

Internet Society. (2000). *History of Internet in Africa*. Available at https://www.internetsociety.org/internet/history-of-the-internet-in-africa/

Kemp, S. (2021). *Digital 2021 Nigeria*. Available athttps://datareportal.com/reports/digital-2021-nigeria

Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). *Social Networking Sites and their Security Issues* (Vol. 3). International Journal of Scientific and Research Publications.

Ogunjobe, O. (2020). *The Impact of Cybercrime on Nigerian Youths*. Retrieved from https://www.researchgate.net/publication/347436728_THE_IMPACT_OF_CYBERCRIME_ON_NIGERIAN_YOUTHS

Olurounbi, R. (2021). *Nigeria Unemployment Rate Rises to 33%, Second Highest on Global List*. Available at https://www.bloomberg.com/news/articles/2021-03-15/nigeria-unemployment-rate-rises-to-second-highest-on-global-list

Petronio, S. (2004). Road to Developing Communication Privacy Management Theory: Narrative in Progress, Please Stand By. *Journal of Family Communication*, *4*(3/4), 193–207. doi:10.120715327698jfc0403&4_6

Premium Times. (2021). *52 Suspected Internet fraudsters Arrested in Benin, Six in Abuja*. Available at https://www.premiumtimesng.com/news/top-news/460807-52-suspected-internet-fraudsters-arrested-in-benin-six-in-abuja.html

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, *91*(1), 93–114. doi:10.1080/00223980.1975.9915803 PMID:28136248

Scroxton, A. (2019). *Three Cyber Criminals Arrested in Nigerian BEC Investigation*. Available at https://www.computerweekly.com/news/252492711/Three-cyber-criminals-arrested-in-Nigerian-BEC-investigation

Tade, O. (2021). *Poverty and Widening Inequality in Nigeria*. Available at https://www.vanguardngr.com/2021/07/poverty-and-widening-inequality-in-nigeria/

The Interpol. (2020). *Three Arrested as INTERPOL, Group-IB and the Nigeria Police Force Disrupt Prolific Cybercrime Group.* Available at https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group

The National News. (2021). *More Than Email Scams: The Evolution of Nigeria's Cyber-Crime Threat.* Available at https://www.thenationalnews.com/world/africa/2021/07/22/more-than-email-scams-the-evolution-of-nigerias-cyber-crime-threat/

The US Department of Justice. (2019). *10 Men Involved in Nigerian Romance Scams Indicted for Money Laundering Conspiracy.* Available at https://www.justice.gov/opa/pr/10-men-involved-nigerian-romance-scams-indicted-money-laundering-conspiracy

Toivo-Think Tank. (2012). *Social Media- The New Power of Political Influence*. Centre for European Studies.

Uba, J., & Agbakoba, O. (2021). *Cybercrimes and Cyber Laws in Nigeria: All You Need To Know*. https://www.mondaq.com/nigeria/security/1088292/cybercrimes-and-cyber-laws-in-nigeria-all-you-need-to-know

Uwem, A., Enobong, A., & Nsikan, S. (2013). Uses and Gratifications of Social Networking Websites among Youths in Uyo, Nigeria. *International Journal of Asian Social Science*, *3*(2), 353–369.

Vanguard Newspapers. (2021). *Nigeria Drops in Transparency International Corruption Perceptions Index, ranks 149 out of 183 countries*. https://www.vanguardngr.com/2021/01/nigeria-drops-in-transparency-international-corruption-perceptions-index-ranks-149-out-of-183-countries/