Netizens' Detection and Mitigation of Crimes in the Digital Environment in Nigeria: A Qualitative Analysis

Desmond Onyemechi Okocha, PhD
Department of Mass Communication
Bingham University, Karu, Nasarawa State, Nigeria
ORCID - 0000-0001-5070-280X
***Email:** desmonddoo@yahoo.com*
and
Michael P. Echoi
Department of Mass Communication
Bingham University, Karu, Nasarawa State, Nigeria
***Email:** mike.echoi@cbnnigeria.org*

Abstract

The Internet and social media have become essential parts of modern life. While this continues to impact speed and quality of delivery positively, one sad problem associated with the technology is cybercrime. This study aims to evaluate the level of cybercrime awareness in Nigeria and find ways to mitigate cybercrimes in Nigeria. Anchored on Technological Determinism and Protection Motivation Theories, the research combines qualitative analysis of relevant literature with primary data collected through a 7-point in-depth interview in which 20 participants were purposively selected from the six geopolitical zones in Nigeria. The study's findings show that Nigerians are well aware of cybercrimes; although Nigeria has legislation to combat cybercrimes, it is ineffective due to a lack of public knowledge. People take action on their own to mitigate cybercrime because the public is unsure of the government's efforts. It is recommended that the government creates job and educational opportunities to discourage would-be criminals, enact effective laws that the public is aware of and penalize defaulters; also that citizens would maintain awareness of information regarding security breaches and use strong passwords that are updated regularly.

Keywords: Cybercrime, cybersecurity, internet use, media literacy, social media.

Introduction

In the last two decades, the Internet and social media have become essential to modern life. University Canada West, [UCW] (2022) opines that social media has taken over industries such as business, advertising, education, and many more; they all rely on the internet and social media as their primary means of communication. According to Saurel (2020), the use of platforms such as Facebook, Twitter, and Instagram has drastically altered how people socialize. People use social media to create, share, and exchange ideas and knowledge in virtual places. The internet has made it possible to hold online lectures, conferences, seminars, workshops, and other events that people can attend from the comfort of their homes (Insegment, 2012). According to Dwivedi, Ismagilova, Rana, and Raman (2021), people nowadays rely increasingly on digital ways of conducting business, and their purchasing process frequently includes using social media. The internet and social media platforms also serve as sources of information and entertainment, such as news, movies, and music.

During the COVID-19 epidemic, the internet's and social media's significance became apparent.

According to Kushner (2020), the world learned that social media is an excellent method for people and communities to stay connected even when physically separated. Kushner maintains that governments and businesses used social media to help people understand what was going on and how it affected them. González-Padilla and Tortolero-Blanco, (2020) say it has never been possible in human history to communicate so swiftly during a pandemic. When people had to work from home, attend lectures online, and have virtual meetings, social media platforms became critical for information dissemination.

Because of the ever-changing nature of technology, the internet and social media have become one of the most rapidly developing and influential mass communication platforms. According to Datareportal (2022), there are 4.65 billion social media users worldwide, accounting for 58.7% of the total global population. Datareportal posits that 326 million new users are added to this figure annually. While the internet and social media technologies have gained widespread adoption and penetration into many parts of human activity, they have also brought their own challenges. It provided new opportunities for criminals by serving as a tool and method for criminals to commit a new type of crime known as cybercrime. Parker (1998) adds that cybercrime is a big worry for the global community. He observes that the introduction, expansion, and exploitation of technologies have boosted criminal activities. In support of this point, Kumar (2022) argues that this poses a substantial commercial risk for practically every corporation, for which many are woefully unprepared. Kumar says that when the crimes include healthcare, the consequences may be more than just financial; they may also result in death.

Cybercrime comes in many forms. Brush (2021) submits that most cybercrimes are committed with the hope of financial benefit by the offenders; nevertheless, others are committed against computers or devices to damage or disable them. Others use computers or networks to spread viruses, illicit information, photos, or other materials.

According to a report issued in 2020 by Cyber Security Ventures, global cybercrime expenses were estimated at $6 trillion USD in 2021. The figure is expected to reach $10.5 trillion per year by 2025.In Africa, according to Emi (2020), as of 2017, cybercrime had cost the African economy $3.5 billion. Nigeria, Kenya, and South Africa suffered annual losses of $649 million, $210 million, and $157 million, respectively, due to cybercrime.

Nigeria is rated 16th among countries afflicted by cybercrime worldwide, with 443 reported cases, according to the FBI's Internet Crime Report (2020). Iwenwanne (2021) avers that Nigeria has over 120 million internet users, and the anti-corruption agency, the Economic and Financial Crimes Commission (EFCC), is facing a cybercrime epidemic in which Nigerians are both victims and offenders. Azeez (2019) further states that various Nigerian corporate companies and individuals lost over $800 million to cyber attacks in 2018. Cybercriminals posing as executives of financial organizations defraud people of their hard-earned money daily. Against this backdrop, this study aims to examine cybercrime in Nigeria to find ways of detecting and mitigating these crimes.

Research Objectives

The objectives of this research are to:

1. Evaluate the level of cybercrime awareness in Nigeria.
2. Evaluate the types of cybercrime existent in Nigeria.
3. Evaluate whether relevant legislation is in place to combat cybercrimes in Nigeria.
4. Find ways to mitigate cybercrimes in Nigeria.

Literature Review

The Menace of Cybercrimes in Nigeria: Causes and Consequences

Cybercrime refers to the use of computers or computer networks as a tool, a target, or a location for illegal activity. It also encompasses classic crimes where computers or networks are utilized to facilitate unlawful activity (Das & Nayak, 2013). The Merriam-Webster dictionary defines Cybercrime as “criminal activity, such as fraud, theft, or distribution of child pornography, committed using a computer especially to illegally access, transmit, or manipulate data”. According to Stam (2020), cybercrimes are crimes perpetrated online and through technology against those who utilize the internet and technology. Security outfits, financial institutions, and businesses worldwide have continued to be compromised through Cybercriminal activities every day. According to Calif (2020), the costs of cybercrime include data loss and damage, money theft, lost productivity, intellectual property theft, theft of personal and financial data, fraud, disruption of routine business operations, forensic investigation, restoration and deletion of compromised data and systems, and reputational harm.

The Federal Bureau of Investigation (FBI) estimates that between 2016 and 2020, there were over 2 million complaints, resulting in a loss of over $13.3 billion due to various cybercrimes. With a total of 443 reported cases, Nigeria was rated 16th among the nations worldwide that were afflicted by cybercrime. Cybercrime, often known as “Yahoo Yahoo” in Nigeria, is one of the most popular types of international crime (Iwenwanne, 2021). The 419 scams, also known as advance fee fraud, is another widespread Cybercrime committed by Nigerians, in which scammers use emails to target persons outside the country's boundaries. Iwenwanne (2021) argues that it is still pervasive to the point that the FBI has a warning on its official website advising against responding to emails from Nigeria requesting personal or banking information.

In recent years, more Nigerians have become victims of internet fraud. According to Ripples Nigeria (2022), research, commercial banks in Nigeria lost a total of ₦15 billion to electronic fraud and cybercrime in 2018, a 53.7 percent increase from the ₦2.37 billion loss reported in 2017. Such figures are terrifying! They beg the question, “What is the cause and motive for Nigerians who perpetrate cybercrime?”

While numerous reasons might be cited, a few stand out.

1. ***Unemployment and Poor Standard of Living*****:** Even after completing their various studies at educational institutions, millions of jobless youths walk the streets, making them susceptible to being victims or perpetrators of cybercrimes. A young person who is unemployed and hungry is typically desperate and would seize every chance to get money to provide themselves with a decent living. These opportunities are usually disguised as internet fraud, or cybercrime.

2. ***Societal Values and Quest for Wealth*****:** Another cause for the rise in cybercrime is the deterioration of social values and the pursuit of wealth. According to Igwe (2021), the growing negative influence of politicians who rise to wealth suddenly by using state resources for private purposes, as well as the fact that no special qualification is required to engage in politics, means that someone can become wealthy overnight if he assumes public office. This get-rich-quick syndrome significantly influences young people who try to achieve it at any cost, including through crime.

3. ***The Ease of Cybercrime*****:** The ubiquity of internet connectivity and the ease of acquiring the tools and gadgets needed to commit cybercrimes also makes it attractive to many, partly because the probability of getting arrested and the cost of investment is low. All a cybercriminal

needs are for one to be online, and one can be attacked from any part of the world. Brush (2021) claims that the criminal no longer has to be physically present when committing a crime. Because of the internet's speed, convenience, anonymity, and lack of boundaries, computer-based versions of financial crimes such as ransomware, fraud, and money laundering, as well as crimes such as stalking and bullying, are easier to commit. In addition, the lack of cybercrime laws to serve as a deterrent to would-be offenders make it easy for the criminals as they often go unpunished.

4. ***Curiosity*****:** Ndubueze (2020) asserts that young people have a natural interest and want to experiment. Some intelligent young individuals may participate in unlawful and deviant online activities due to this curious thinking. Just for the fun of it, they might try to enter someone else's account by guessing passwords, for instance.
   Whatever the motivations, Nigerian cybercrime trends have far-reaching consequences for corporations, government institutions, educational systems, and the general population. Some of these effects are discussed below.

5. ***Foreign Investors*****:** Due to the nation's negative reputation, foreign investors are discouraged and scared off. A nation's reputation is damaged in the eyes of the international community when there is a high level of cybercrime. Nigerian Communications Commission [NCC] (2017) asserts that this directly impacts the nation's unemployment rate when foreign investors and their parent companies leave the country and, in some cases, reduce staff numbers as a result of cyber attacks that have caused a decline in profit.

6. ***Impact on Productivity*****:** People regularly transact businesses online in the digital age; as a result, cyber security costs as part of a company's annual budget is becoming obligatory. This significantly reduces the overall productivity of enterprises and organizations because significant resources are now directed toward acquiring hardware and software to defend systems against assaults. Companies typically spend between 7.2 percent and 15.2 percent of their IT expenditures on cyber security each year, according to Lemos (2020). Many man-hours are also lost in adopting security measures that could have been employed to increase profit. According to a Nigeria Communication Commission, NCC (2017) report, people spend more time preventing, diagnosing, or protecting themselves from the repercussions of cybercrime than they are engaged in more productive activities. Employees must input different passwords and undertake other time-consuming tasks to complete their work for the day. Every second spent on these duties is a second not spent working productively.

Cases of Cybercrimes in Nigeria

Every day in Nigeria, numerous cybercrimes are perpetrated. Ladipo (2022) posits that there are 2,308 attacks on businesses weekly in Nigeria, spanning all industrial sectors. Many go unreported because they are unnoticed or impossible to track by the authorities. Some have gained attention, and the offenders have been prosecuted. The following lists a few examples:

1. On March 10, 2018, a group of seven hackers in Lagos used malware to steal N900 million (US$24,000) from a single bank (Ripple Nigeria, 2022).

2. According to Iwenwanne (2021), in 2019, the FBI arrested 77 Nigerian people, including high-profile entrepreneur Obinna Okeke, for involvement in an enormous internet financial fraud scam totaling about $11 million.

3. In June 2020, Hushpuppi, a 37-year-old male, was apprehended in a raid in Dubai and later deported to the US. He was detained for allegedly laundering millions of dollars from fraud, cybercrimes, and attempts to defraud an English Premier League club out of £100 million ($125.5 million) (Maxwell, 2020).

4. According to the Thisday newspaper (2021), the Nigerian Economic and Financial Crimes Commission (EFCC) reported the arrest of more than 400 young Nigerians for internet-related fraud in the first three months of 2021.

5. In a joint operation with INTERPOL, the Nigerian Police Force (NPF) captured 11 alleged members of an extensive cybercrime network between the 13th and 22nd of December, 2021. Many of the suspects are said to be members of the 'SilverTerrier' network, which is notorious for Business Email Compromise (BEC) crimes that have harmed thousands of firms around the world (INTERPOL, 2022).

6. The Federal High Court in Ilorin sentenced three people with cybercrime-related charges on April 7, 2021 (TheGuardian, 2022).

7. On September 2, 2020, EFCC agents arrested 13 persons suspected of belonging to an organized cyber-criminal gang that defrauds unsuspecting victims out of millions of Naira (Ogbonnaya, 2020).

8. The US Attorney General's Office in California indicted 80 people in October 2019 on suspicion of fraud and money laundering violations totaling $46 million. Of the 80 accused, 77 were of Nigerian origin (AFP, 2019).

9. According to a news statement issued by the Economic and Financial Crimes Commission EFCC (2021), two people, Tobilola Bakare and Alimi Sikiru were convicted of cybercrime on August 9, 2021. Through Business Email Compromise fraud, the hackers successfully robbed three airlines, KLM, Turkish Airlines, and British Airways, of a total of $1 million.

10. On March 27, 2021, the Economic and Financial Crimes Commission (EFCC) detained a young man, Ibeh Theophilus Uche, and his mother in Lagos for their suspected involvement in computer-related fraud totaling N50 million (Ogune, 2021).

11. On 28 January 2020, a Federal High Court in Lagos convicted Damilola Ahmed Adeyeri and his mother, Alaba Kareem Adeyeri, of $82,570 in cyber-related fraud (Sunday & Ogune, 2020).

12. Azeez Bamidele, a newlywed man, was sentenced to six months in prison by an Ikeja Special Offences Court in Lagos State on June 10, 2020, for internet fraud (Sunday, 2020).

13. According to the News Agency of Nigeria, NAN (2017), on May 15, 2017, two siblings, Chukwudi Ugwueke and Sophia Ugwueke, were convicted to two years in prison each for internet fraud in Warri, Delta state. They were convicted of unlawful conduct bordering on scamming foreigners via internet frauds.

14. On September 23, 2016, the Economic and Financial Crimes Commission (EFCC) arrested two people, ages 26 and 29, who were involved in various internet fraud operations such as impersonation and internet love and romance scams (NAN, 2016).

15. According to TheCable (2021), eight Nigerians were arrested in October 2021, and are to face charges in the United States for alleged online fraud. The suspects and other conspirators were said to have collaborated from Cape Town to engage in massive internet fraud involving romance scams and advance fee schemes between 2011 and 2021.

Government and Legislative Response to Cybercrimes in Nigeria

According to United Nations Conference on Trade and Development, UNCTAD (2021), cybercrime is an increasing threat to countries at all stages of development, affecting buyers and sellers. United Nations Office on Drugs and Crime, UNODC (2017) adds that the complexity of cybercrime underscores the necessity for an immediate, dynamic, and global response. Governments worldwide are attempting to develop laws to prevent and combat cybercrime.156 nations have passed cybercrime legislation, according to UNCTAD (2021); however, the distribution varies by area. Europe has the highest rate of adoption, whereas Africa has the lowest.

Uba (2021) asserts that the Cybercrimes (Prohibition, Prevention, and Punishment) Act of 2015 was passed and took effect on May 15, 2015, based on the idea that threats to information and communication technology pose a challenge to Nigeria’s national security and have an impact on the nation's economic, political, and social fabric. Imue (2021) posits that the Act's primary goal is to give Nigeria a practical institutional, legal, and regulatory framework for prohibiting, preventing, detecting, and prosecuting cybercrimes. The Act also aims to advance cyber security and the defense of electronic communications, data and computer programs, computer systems and networks, intellectual property, and privacy rights. The Federal Ministry of Justice and the Economic and Financial Crimes Commission (EFCC) are the two central prosecuting agencies under the Act. Other vital participants include government organizations and private-sector companies, although the National Security Adviser is in charge of overall national cyber security actions (Uba, 2021).

According to Nigerian Computer Emergency Management Team, ngCERT (2021), the Cybercrime Advisory Council (CAC) was set up to coordinate the Cybercrime Act 2015 and was given the duty of developing general policy guidelines for preventing and combating cybercrimes as well as facilitating cyber security in Nigeria. Uba (2021) adds that CAC was established in March 2016 in compliance with Articles 42 and 43 of the Cybercrimes Act, with members representing a wide range of ministries and agencies reporting to the National Security Adviser.

Other legislation has been proposed in addition to the Cybercrimes (Prohibition, Prevention, and Punishment) Act of 2015. For example, the National Assembly is now debating a draft Data Protection Bill 2020.According to PwC (2020), Bill's goal is to establish a legal framework for the protection and processing of personal data and to preserve data subjects’ constitutionally protected rights and liberties. Uba (2021) posits that the National Assembly approved the Data Protection Bill in 2019, but the President did not sign it. The law was resubmitted to Parliament for approval after the presidential elections, and it is currently being resumed to continue the legislative process.

Review of Empirical Studies

Ahern, Feller and Nagle (2016) conducted a study on social media as a support for learning in universities: an empirical study of Facebook

Groups; with the central objective of specifically creating an understanding of what motivates university students to use Facebook in their academic activities. Using the Student Technology Use Hierarchical Framework, which is drawn from the Uses and Gratifications Theory and the Means-End Chain Theory, the survey drew 260 responses representing 53% of the population which comprised undergraduates. Part of the findings showed that these students love social media generally but preferred Facebook Group because if its interactive nature, which they claimed satisfies their higher-level information exchange and decision-making requirements. Irrespective of which platform is preferred, the result generally indicates that social media have become useful tools in academic development among students.

Moon, McCluskey and McCluskey (2010) in a study on the general theory of crime and computer crime, explained computer crimes using the self-help computer theory. With a sample population of 2,751, they collected data from a nationally representative population of Korean adolescents and their parents to understand various issues; Korean youths experience; for example, in the area of cybercrime and fear of crime. Their findings indicate that in line with the theory's suggestion, long hours of computer use made the users vulnerable to computer crimes. This is because of the intense curiosity and information on discoveries shared by other classmates.

In a study by Bossler and Berenblum (2019) on the introduction of new directions in cybercrime research aimed at categorizing the different aspects of the menace called cybercrime, the authors, based on their findings, concluded that it was merely impossible to compute the number of cybercriminal acts that occur across the world, from cyber trespass to cyber deception, which include identity theft, online fraud, digital piracy; cyber porn/obscenity or what they call child sexual exploitation material, and cyber violence. The scope keeps expanding.

Ahmad, Wisdom and Isaac (2020) conducted an empirical analysis of cybercrime trends and their impacts on moral decadence among secondary school students in Nigeria, with the objective of establishing the depth of students' involvement in crime in Nigeria and their vulnerability. The research focused on two states—Kebbi and Sokoto. They administered questionnaires to the students at home, away from the influence of their teachers. The study revealed ages, the number of social media accounts each of them had, how often they visited pornography sites and their knowledge of the internet. Although the study does not present the sample size and the theoretical framework adopted, it is used to confirm the fact that "students at almost all academic levels" are in different ways involved in cybercrime in Nigeria.

Omodunbi, Odiase, Olaniyan and Esan (2016) have examined cybercrimes in Nigeria: analysis, detection and prevention. The objectives were to analyze cybercrimes carried out in prominent sectors in Nigeria and present a brief analysis of cybercrimes in tertiary institutions in Ekiti State. They evaluated the extent of students' involvement in the crime to determine the level of their vulnerability in such situations. Three universities were chosen, and 600 students were sampled in questionnaires with 15 questions. The results showed that most students spent more time on social media platforms. Without admitting to the crime, 81% of the respondents replied that cyber crimes were usually executed from home; and 88% said they had been victims of cybercrime known as 'phishing'. One significant finding of the research was that cybercrimes are principally carried out by the youth who spend a long time on the internet.

Lazarus (2016), in a study on socioeconomic cybercrimes in Nigeria, came up with some revelations. The study aimed at exploring parents' perceptions of the numerous issues that lead to socioeconomic cybercrime in Nigeria, examining how a child's family environment could shape and determine the child's behaviour; and how this can help in combating cybercrime among juveniles. Adopting the qualitative methodology, the study covered 17 parents. It administered in-depth semistructured questions involving face-to-face interviews. Responses were then coded. Findings showed that a good family environment, a broken home, the culture of the home, parental upbringing, corruption, peer group and university environment, were cited by parents as factors that determine a child's criminal attitude. The conclusion was that a child's susceptibility to involvement in cybercrime activities would be determined by the depth of that child's exposure to influences posed by these factors.

Theoretical Framework

According to Nuth (2008), the development of information and communication technologies (ICTs) has a significant impact on crime; it increases the number of opportunities for corruption and encourages criminal behavior, causing crime to rise at an unprecedented rate. Europol (2017) reports that while several technological advancements play a significant part in a broad spectrum of criminal activities, none has probably had a more significant impact or influence than the internet. Each year, criminal organizations and individuals continue to make billions of Euros from their operations in the EU. Also, Bavel *et al*. (2019) reason that social engineering attacks are now commonplace and considered one of the most significant threats to organizations and individuals. They argue that researchers and security professionals have reported that human behavior is the 'weakest link' in any security chain. Based on these arguments, therefore, this study is anchored on Technological Determinism Theory and Protection Motivation Theory. While Technological Determinism Theory helps with seeing how advances in technology impact current trends of crime in society, Protection Motivation Theory will help evaluate people's protection behavior under the threat of cybercrime.

According to Marshall McLuhan's 1964 theory of Technological Determinism, as we advance from one technological age to another, technology impacts how each member of society thinks, feels, and behaves and how society functions. In Asemah (2011), McLuhan believes that technological inventions cause cultural changes. According to Jan, Khan, Naz, Khan, and Khan (2021), McLuhan divided human cultures into four eras: the tribal age, the literate age, the print age, and the electronic age. The tribal period was followed by the literate age, which gave way to the print age, which then gave way to the era of electronic communications. The day's technology transformed people's lifestyles according to their respective ages. For instance, the rise of industrial civilization was facilitated by the discovery of steam power, and the information era was ushered by the invention of computers and the internet (Theory, 2022).

Protection Motivation Theory (PMT) was first introduced by Rogers (1975), to understand better the effects of fear appeals on health-related attitudes and behavior. In 1983, Rogers revised the theory with an emphasis on the cognitive processes of mediating behavioral change. The Protection Motivation Theory deals with how people cope with and make decisions in times of harmful or stressful events in life. According to Rajendran & Shenbagaraman (2017), PMT claims that four things impact a person's intent to protect them from dangerous or hazardous occurrences. (i) the severity of the harmful or threatening event (perceived severity), (ii) the likelihood of the event occurring (vulnerability), (iii) the effectiveness of the planned preventive steps (response efficacy), and (iv) the ability of the person in executing the plan to reduce the effect of a threatening event (self-efficacy).

The threat appraisal (perceived severity and vulnerability) indicates the degree of significance of the event. Higher threat appraisal indicates a decreased likelihood of maladaptive behavior. The coping appraisal (response efficacy and self-efficacy) focuses on the adaptive responses; it determines a person's ability to cope with a threat and take steps to avoid it. Bavel, Rodríguez-Priego, Vila, & Briggs (2019) opines that strong threat appeals, when presented alone, are ineffective. In contrast, strong threat appeals presented in combination with coping messages have produced the most significant behavioral change, despite the associated response costs.

The justification for anchoring the study, first on Technological Determinism Theory is that in every generation, each technology determines the behaviour of the society, especially the youth. As explained by Asemah (2011), the culture or way of life of the people in a given era is influenced by a subsisting technology. In this particular study, this theory establishes how the internet technology determines the behavioural pattern of Nigerian Netizens. The relevance of the second theory, the PMT, is based on the fact that cybercrime affects both the victims and the morals of the society. The theory explains and analysis steps taken by the security system and the would-be victims to safeguard the public and individuals against cybercrime threats.

Research Method

The study combined both qualitative analysis of relevant literature with primary data gathered from 20 participants in a 7-point in-depth interview. This approach was deliberately adopted to enrich the data contents of the study. The participants were purposively picked from the six geopolitical zones of Nigeria. As a country with more than 250 ethnic groups, Nigeria is divided into six geo-political zones. Picking participants from the zones therefore means that every part of the country is represented in the research. Among the participants were business owners, students, civil servants, journalists, and social workers. They cut across different age brackets. The youngest was 16 years while the oldest was over 50. The secondary data for the study were assembled from extant scholarly literature and outcome of various empirical studies published on the subject matter in reputable academic journals.

Data Analysis

The following tables provide details for Socio-Demographic, Social Media presence, and Social Media usage, respectively.

Q1: Demographic Distribution

Table 1: Socio-Demographic Details

Location	**Frequency**	**%**
North Central	4	25
North East	3	10
North West	3	15
South South	3	15
South East	3	15
South West	4	20
TOTAL	20	100
Occupation	**Frequency**	**%**
Business Owners	3	15
Students	4	20
Civil Servants	5	25
Journalists	4	20
Social Workers	4	20
TOTAL	20	100
Age Range	**Frequency**	**%**
16 – 20	2	10
21 – 30	4	20
31 – 40	9	45
41 – 50	3	15
51 and above	2	10
TOTAL	20	100

Source: Field Study, 2022.

Table 1 above has three sub-tables that deal with the demography of the respondents — from age to gender, occupation, and geographical locations. The first sub-table indicates in the first column, the six geo-political zones where the participants stay. The second column states the study population in each of the zones while the third column shows the percentages of samples.

The second sub-table shows the occupations of respondents from each of the geo-political zones and the percentages. While civil servants top the list with 25%, students, journalists and social workers were 20% each, and business owners was third with 15% of the total number of participants. The age differences among the respondents are displayed in the last sub-table. It shows the age range, the number of respondents within each of the age brackets and the percentages. The lowest age bracket is between 16 and 20, while the highest is between 50 and above.

Table 2: Social Media Presence (Various Social Media Platforms)

Platform	**Presence**	**Platform**	**Presence**
Facebook	19	Snapchat	2
Instagram	15	TikTok	1
YouTube	6	Reddit	1
WhatsApp	19	Amazon	1
Telegram	6	Aliexpress	1
Linkedin	7	Jumia	1
Twitter	10	Konga	1
Google Meet	1	Medium	1
Zoom	1	Messenger	1
Signal	1		

Source: Field Study, 2022.

Table 2, displays, in four columns, the different social media platforms patronized by the respondents. In all, 19 social media platforms are indicated. Facebook and WhatsApp platforms attracted the highest patronage of 19 out of the 20 participants in each case. This demonstrates the popularity of the two platforms. Instagram and Twitter polled 15 and 10 participants, respectively, while Linkedin, YouTube, and telegram were patronized by 7, 6 and 6 participants, respectively. Apart from Snapchat, which had two persons, other social media platforms had patronage from one person each.

Table 3: Social Media Usage (Frequency of Usage)

Intensity of Use	**Frequency**	**%**
All Day	0	0
6 - 15 hours	5	25
3 - 5 hours	9	45
1 - 2 hours	3	15
Sparingly	3	15
TOTAL	20	100

Source: Field Study, 2022.

Under Table 3, each respondents' usage of the social media platform is measured. These are expressed in numbers and also in percentages. Among the respondents, 25% said they spend between 6 and 15 hours on the social media a day; and 45% spent between 3 and 5 hours. While 15% of the respondents are on the social media for a maximum of two hours daily, another 15% of the population said they use the platforms sparingly. As would be seen under Discussion, the longer the number of hours people are exposed to the use of the social media, the more vulnerable they are regarding exposure to certain criminal acts associated with the cyber world.

Table 4: Activities people engage with on social media

Activities	**Frequency**
Entertainment	11
Networking/Socializing	12
Information gathering/news	8
Messaging	4
Commerce/Banking	10
Communication/Meetings	7
Education	6

Source: Field Study, 2022.

Table 4 displays individual responses to what each participant seeks on the social media. Among them, 12 persons confirmed that they patronized the social media for networking or social reasons, while 11 participants claimed that they visit the different social media platforms for entertainment.

Ten participants said their social media patronage was for business involving banking and commerce; eight said they did so in search of information and news, while seven persons mentioned communication and meetings as reasons for their patronage. In all, six persons said they were usually on social media for educational purposes, while four persons said they were there for messaging.

Q2: Knowledge, use of social media and awareness of cybercrime

All 20 participants admitted that they were familiar with and use of various social media platforms, including Facebook, WhatsApp, Twitter, Instagram, YouTube, Zoom, and many others, as seen in table 2 above. While the frequency of usage varied from one participant to another, it was observed that participants could be easily grouped from sparing users to heavy users. People, on average, spend between 3 hours to 5 hours daily on social media, as illustrated in table 3. This indicates the depth of pull that social media have on people generally, using this population as an example. Social media have become an irresistible phenomenon across age barriers.

On what exactly they do while on the social media platforms, participants indicated that they use social media for a wide range of activities, including but not limited to entertainment, as sources of news and information, networking and socializing, messaging, commerce/banking, and education. Networking and socialization, entertainment, and commerce/banking showed to be the highest activities participants use social media for in Table 4 below. These findings, on close examination, showed that most of what is coded as entertainment could be pornography and cyber sexual adventures. At the same time, networking and socialization, commerce and banking, could actually refer to activities that are criminal in nature.

These assumptions were confirmed when all the participants, individually, said they were aware of the booming cybercrimes business like Identity theft, Romance Scam, Business Email Compromise, Cyberbullying, Pornography, Fake News, Financial Frauds (Yahoo, yahoo), and Phishing. The most resonant with them are Identity Theft, Business Email Compromise, and Financial Fraud. Meanwhile, of the 20 participants, 16 have had an experience or know someone close to them who has had one. A few of their experiences are highlighted as follows:

> A woman I worked with who lives in the UK was in a relationship with a Nigerian who impersonated a white man and duped her of 75 pounds. (P-6).

> My ATM details were obtained from a website I made a purchase from. The hacker used the

> information to make purchases from another website. (P-16).
>
> A friend has duped 300,000 Naira while trying to make an online payment and was asked to click on a link. (P-18).

Q3: Actions people take when attacked

After admitting that they were aware of cybercrimes and the fact that some of them have been victims, participants said they have learnt to apply various actions and defense options when they come under cyber attacks. They do these in order to mitigate future occurrences. One of them said they moved their fund from the hacked account to a safe account and disabled the functionality of the hacked account. Another participant said they changed the security settings of their accounts and created limited access to such accounts. Other actions include activating double authentication settings of affected accounts, sending out messages to contacts and asking them to disregard malicious contents from the hacked account, reporting to the police; blocking all debiting on the account through the bank's app; and re-issue of affected ATM cards. One participant said;

> I deleted the app and stayed off it for over two years (Facebook). (P-3).

All these confirmed that either as a victim or participant in cybercrime, participants are fully aware of the threats, the execution and the consequences of cybercrime. Some might be lured into the crime while others fortify themselves against such crimes.

Q4: Awareness of existing cybercrime laws and their effectiveness

The reason a negligible percentage of the participants said they sometimes reported the threat and actual cybercrime act to the police is that they are aware of existing laws against the act. In all, 14 out of the 20 participants said they were unaware of any existing legislation for combating cybercrime in Nigeria. Only 4 participants said they were aware of the Cybercrime Act 2015, but out of these number, a participant said;

> Yes, but there is hardly any publicity or promotion of the said law considering the rate at which cybercrime happens. (P-18)

Both those who are aware of existing laws and those who said they were not, agreed that no such law was sufficiently effective to combat the rising cybercrime wave. It is either they have been involved in the crime and the law could not prevent them, or they have been victims who have found the law not combative enough to protect them. According to a participant;

> The law has empowered the police, Economic and Financial Crimes Commission, EFCC, and other law enforcement agencies to tackle cybercrime. Still, it appears that the law has not effectively reduced cybercrime. (P-3).

Q5: How cybercrime can be minimized

All the participants expressed loss of confidence in any existing law in Nigeria meant to eradicate or even reduce cybercrime from the system. The only panacea, according to them, is for individual victims or those facing threats of attack to fortify their accounts against any such attack. Participants reasoned that cybercrimes could be minimized through the use of strong passwords that are frequently changed by account owners, minimal sharing of personal information online, reduction of online transactions, and investing in cyber security tools and recovery software. But none of them forgot that some people with multiple online social media accounts would find it difficult to sustain different passwords required to keep those accounts safe. The suggestion to reduce online transactions, including banking, also faced reservations even from those who suggested it. Curiously, no participant strongly recommended further legislation by the government or expressed any confidence in the ability of law enforcement agencies to combat cybercrime successfully in Nigeria.

Discussion

The first objective of the research was to evaluate the level of cybercrime awareness in Nigeria. The survey finds that every participant in the interview has a presence on many social media platforms, which has an impact on a variety of elements of their lives, including communication, networking, and information and news sources. This is equally confirmed by the findings in an empirical study by Ahmad, Wisdom and Isaac (2020) in which all the students questioned had several social media platforms, which they visit regularly. Smitherson (2012) supports this claim by stating that there is no doubt or room to refute the successful impact of these social media platforms on our daily lives, professional lives, and even business. The data also backs up Marshall McLuhan's idea of Technological Determinism, which holds that technology influences how each member of society thinks, feels, and behaves, as well as how society functions as a whole. Despite social media's many advantages for society today, according to Onadipe (2021), it is also a haven for cybercriminals looking for unwary victims. All participants who were interviewed agreed that they were aware of crimes involving social media, which lends credence to Onadipe's assertion.The study by Omodunbi *et al*. (2016) also showed that 88% of respondents agreed that they have been victims of cybercrimes, especially phishing.

The second objective of the research was to evaluate the types of cybercrimes in Nigeria. While participants interviewed mentioned identity theft, romance scam, business email compromise, cyberbullying, pornography, fake news, financial frauds (yahoo, yahoo), and phishing as common cybercrime perpetrated in Nigeria, they think that identity theft, business email compromise, and financial fraud are the most prevalent. Bossler and Berenblum (2019) in their study confirmed this pattern of cybercrime across other climes, including Nigeria. Iwenwanne (2021) supports this view by submitting that identity theft, business email compromise, and financial fraud are still pervasive to the point that the FBI has a warning on its official website advising against responding to emails from Nigeria requesting personal or banking information. According to a recent ThisDayLive article, Aragba-Akpore (2022) stated that the Economic and Financial Crimes Commission (EFCC) stormed a "419 training school" in Lagos in May 2019 and arrested the proprietor as well as eight students who were allegedly being taught techniques to commit cyber fraud. In addition, on May 12, 2022, the Commission arrested the owner of a "yahoo yahoo" academy in Abuja during a sting investigation.These trends indicate that identity theft, company email compromise, and financial fraud are on the rise.

The third objective of the research was to evaluate if relevant legislation is in place to combat cybercrimes in Nigeria. The study discovered that the government had enacted legislation to combat cybercrime, the Cybercrime Act 2015. However, only four (4) of the twenty (20) people interviewed were aware of it. One of the participants who were familiar with the law claimed that, given the frequency of cybercrime, there is hardly any exposure or promotion of the relevant law (P-18).Another participant (P-3) acknowledges that the law has empowered the Police, Economic and Financial Crimes Commission, EFCC, and other law enforcement agencies to tackle cybercrime but that the law has not been effective in reducing cybercrime. To support this claim, Aragba-Akpore (2022) says that although the legislation is supposed to control the rising crime rate, surprisingly, young people are still involved in it.

The fourth objective of the research was to find ways to mitigate cybercrimes in Nigeria. In addition to its consequences of data loss and damage, money theft, loss of productive time, intellectual property theft, theft of personal and financial data, fraud, and reputational harm (Calif, 2020), cybercrime, according to Rainer Bohme and Moore (2012), threatens to impose even higher opportunity costs by discouraging online involvement for fear of becoming victims. This agrees with Brands and van Wilsem (2019), who argue that fear of online crimes can limit people's perceptions of online freedom and possibilities. According to Johansen (2020),

> When you hear and read about the range of cybercrimes out there, you might be tempted to stop using the internet entirely. That's probably too drastic. You can, however, take precautions to help protect against it.

According to the Prevention Motivation Theory, the threat of a bad outcome sets off two separate parallel cognitive processes called threat appraisals and coping appraisals. One's motivation to protect is higher when the appraisals are stronger. The study reveals that the threat of cybercrime is real enough to elicit people's coping responses. However, Omodunbi *et al*. (2016) suggest in their study that mitigating the occurrence of cybercrime can be achieved if the government focuses on improving the welfare and well-being of Nigerians, especially the young ones. In addition, they believe that the youth should be properly educated and orientated on the avoidable negative impacts of the business.

While it is unclear to participants what steps the government is taking and whether those activities are sufficient to reduce cybercrime in Nigeria, people indicate that they have put various measures in place to protect themselves from cybercrime threats. Some of the steps people take include moving money from a compromised account to a safe account and shutting down the compromised account's functionality, changing account security settings and limiting access to such accounts, turning on double authentication settings for affected accounts, sending out messages requesting that contacts ignore malicious content sent to them from a compromised account, and reporting cyber attack cases to the Police.

Conclusion

The impact of technology on society has resulted in both possibilities and challenges. While technology continues to positively impact many aspects of human endeavour, including communication, education, commerce, and many other fields in the speed of delivery and product quality, one sad problem of technology is cybercrime. The study's findings showed that Nigerians are well aware of cybercrime; identity theft, business email compromise, and financial fraud are Nigeria's most common types of cybercrime. Although Nigeria has legislation to combat cybercrime, it is ineffective due to a lack of public knowledge. People appear to take action to reduce cybercrime because the public is unsure of the government's position. It is proposed that additional study is required in order to fully understand the Nigerian government's initiatives in this regard.

Recommendations

Cybercrime prevention involves ongoing government, corporate institutions, and individual strategy changes. The following are recommendations for preventing cybercrimes in Nigeria:

i. Nigerian citizens should use strong passwords that are updated regularly.
ii. The public should be constantly kept aware of information regarding security breaches.
iii. Government should create jobs and educational opportunities for the youth to prevent them from looking in the direction of crime.
iv. The government should enact effective laws that the public is aware of and penalize criminals.
v. The glamourization of money with unknown sources should be discouraged in society.

References

Agence France-Presse, AFP. (2019, September 10). *FBI and Nigeria step-up cyber-crime investigations*. Accessed from https://guardian.ng/news/fbi-and-nigeria-step-up-cyber-crime-investigations/

Ahern, L., Feller, J., & Nagle, T. (2016). Social media as a support for learning in universities: an empirical study of Facebook Groups. Journal of Decision Systems, 25(1), pp: 35-49. Accessed from https://doi.org/10.1080/12460125. 2016.1187421

Ahmad, M. A., Wisdom, D, D., & Isaac, S. (2020). An empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. https://doi.org/10.22624/iSTEAMS/V26P10-IEEE-NG-TS

Asemah, E. S. (2011). *Selected Mass Media Themes.* Jos University Press.

Aragba-Akpore, S. (2022, July 16). *Digital Literacy and Rising Cybercrimes*. Accessed from https://www.thisdaylive.com/index.php/2022/06/01/digital-literacy-and-rising-cyber-crimes/

Azeez, O. (2019, December 3). *Cyber crime cost Nigeria N288bn in 2018*. Accessed from https://www.businessamlive.com/cyber-crime-cost-nigeria-n288bn-in-2018/

Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019, March). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123*, 29-39.

Bossler & Berenblum (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice, 42*(5), pp: 495-499. Accessed from https://doi.org/10.1080/0735648X.2019.1692426

Brands, J., & van Wilsem, J. (2019). *Connected and fearful?* Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*.

Brush, K. (2021, September). *Definition cybercrime*. Accessed from https://www.techtarget.com/searchsecurity/definition/cybercrime

Calif, S. (2020, November 13). *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*. Accessed from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Das, S., & Nayak, T. (2013, October). Impact of Cyber Crime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies, 6*(2), 142-153.

Datareportal. (2022, May 1). *Global Social Media*. Accessed from https://datareportal.com/social-media-users

Dwivedi, Y. k., Ismagilova, E., Rana, N. P., & Raman, R. (2021, February 02). Social Media Adoption, Usage And Impact In Business-To-Business (B2B) Context: A State-Of-The-Art Literature Review. Information Systems Frontiers (2021). Accessed from https://doi.org/10.1007/s10796-021-10106-y

EFCC. (2021, August 9). *Court orders forfeiture of internet fraudsters' three duplexes, 200 million, luxury cars*. Accessed from https://www.premiumtimesng.com/news/top-news/478405-court-orders-forfeiture-of-internet-fraudsters-three-duplexes-200-million-luxury-cars.html

Emi, I. (2020, December 3). *Cybercrime costs Africa billion of dollars per*. Accessed from https://venturesafrica.com/cybercrime-costs-africa-billons-of-dollars-per-year/

Europol. (2017). *Europol Unclassified – Basic Protection Level.*

Federal Bureau of Investigation FBI. (2020). Internet Crime Report.

González-Padilla, D. A., & Tortolero-Blanco, L. (2020). Social media influence in the COVID-19 Pandemic. *International Brazilian Journal of Urology*, 120-124.

Igwe, U. (2021, June 9). *Nigeria's growing cybercrime threat needs urgent government action*. Accessed from https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/

Imue, M. (2021, April). *The Jurisdiction Challenge in the Enforcement of Cybercrime Laws in Nigeria*. Accessed from https://www.alp.company/resources/business-advisory/jurisdiction-challenge-enforcement-cybercrime-laws-nigeria

Insegment. (2012, June 25). Reliance on social media in today's. Accessed from https://www.insegment.com/blog/reliance-on-social-media-in-todays-society/

INTERPOL. (2022, Jnuary 19). *Nigerian cybercrime fraud: 11 suspects arrested, syndicate busted*. Accessed from https://www.interpol.int/en/News-and-Events/News/2022/Nigerian-cybercrime-fraud-11-suspects-arrested-syndicate-busted

Iwenwanne, V. (2021, July 22). *More than email scams: the evolution of Nigeria's cyber-crime threat*. https://www.thenationalnews.com/world/africa/2021/07/22/more-than-email-scams-the-evolution-of-nigerias-cyber-crime-threat/

Jan, A., Khan, S. A., Naz, S., Khan, O., & khan, A. Q. (2021). Marshal McLuhan's Technological Determinism Theory in the Arena of Social Media. *Pakistan Journal of Social Sciences, 18*(Issue 2), 30-34.

Johansen, A. G. (2020, September 30). *11 ways to help protect yourself against cybercrime*. Accessed from https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html#

Kumar, S. (2022, March 3). *Cybercrime: A clear and present danger*. Accessed from https://www.securitymagazine.com/articles/97190-cybercrime-a-clear-and-present-danger#:~:text=Business%20Risk,-Today%20all%20significant&text=Recent%20shifts%20to%20cloud%2Dbased,data%20loss%20and%20ransomware%20demands.

Kushner, J. (2020, March 25). *The role of social media during a pandemic*. Retrieved from https://khoros.com/blog/social-medias-role-during-covid-19

Ladipo, E. (2022, January 14). *Nigerian businesses suffer 2308 cyber attacks every week*. Accessed from https://businessday.ng/technology/article/nigerian-businesses-suffer-2308-cyber-attacks-every-week/

Lazarus, S. (2016). Causes of socioeconomic cybercrime in Nigeria (Conference session). International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, Canada. https://doi.org/10.1109/ICCCF.2016.7740439

Lemos, R. (2020, August 5). *Cybersecurity Budget Rose in 2019, Uncertainty Prevails in 2020*. Accessed from https://www.darkreading.com/operations/cybersecurity-budget-rose-in-2019-uncertainty-prevails-in-2020

Maxwell, C. (2020, December 28). *From Hushpuppi to crystal meth gangs, Dubai Police's highest profile busts of the year*. https://www.thenationalnews.com/uae/courts/from-hushpuppi-to-crystal-meth-gangs-dubai-police-s-highest-profile-busts-of-the-year-1.1136025

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. Journal of Criminal Justice, 38(4), pp: 767-772. https://doi.org/10.1016/j.jcrimjus.2010.05.003

News Agency of Nigeria, NAN. (2016, September 23). *EFCC arrests 2 in Ibadan over* *internet fraud*. https://guardian.ng/news/efcc-arrests-2-in-ibadan-over-internet-fraud/

News Agency of Nigeria, NAN. (2017, May 15). *Court jails 2 siblings for Internet fraud*. Accessed from https://guardian.ng/news/court-jails-2-siblings-for-internet-fraud/

Nigerian Communications Commission, NCC. (2017). *Effects of Cyber Crime on Foreign Direct Investment and National Development.* Nigerian Communications Commission.

Ndubueze, P. N. (2020, February). Causes and Consequences of Cybercrime in.

ngCERT. (2021). *About the cybercrime Advisory*. https://www.cert.gov.ng/cac

Nuth, M. S. (2008, December). Taking advantage of new technologies: For and against crime. *Computer Law & Security Review*, 437-446.

Ogbonnaya, M. (2020, October 19). *Cybercrime in Nigeria demands public-private action*. Accessed from https://issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action

Ogune, M. (2021, March 27). *EFCC arrests son, mother for N50m internet fraud*. Accessed from https://guardian.ng/news/efcc-arrests-son-mother-for-n50m-internet-fraud/

Omodunbi, B., Odiase, P. O., Olaniyan, O., & Esan, A. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology,* 1(1), pp: 36-42. https://doi.org/10.46792/fuoyejet.v1i1.16

Onadipe, R. (2021, May). *Impact of social media on cyber crime in today's digital age*. Accessed from https://www.thecable.ng/impact-of-social-media-on-cyber-crime-in-todays-digital-age#:~:text=Common%20examples%20of%20cyber%20crime,sharing%20ideas%20and%20expanding%20businesses.

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information.*

PricewaterhouseCoopers, PwC. (2020). *The NDPR and the Data Protection Bill 2020*. Accessed from https://www.pwc.com/ng/en/publications/data-protection-bill-2020.html

Rainer Bohme , & Moore, T. (2012). How do consumers react to cybercrime? *eCrime Researchers Summit (eCrime), 2012.*

Rajendran, S., & Shenbagaraman, V. (2017). A Comprehensive Review of the Applications of Protection Motivation Theory in Health Related Behaviors. *Journal of Chemical and Pharmaceutical Sciences, 10*(1).

RipplesNigeria. (2022, June 10). *Investigation: How online fraudsters siphon victims' funds through*. Accessed from https://www.ripplesnigeria.com/investigation-how-online-fraudsters-siphon-victims-funds-through-sportybet-platform/#:~:text=In%202018%2C%20commercial%20banks%20in,billion%20loss%20recorded%20in%202017.

Saurel, S. (2020, Feb 10). *The impact of social media on our society*. Retrieved June 2022, from https://www.mediaupdate.co.za/social/147946/the-impact-of-social-media-on-our-society

Smitherson, D. (2012, Nov 14). *Impact of Cyber Crime and Security on Social Media*. Accessed from https://www.socialmediatoday.com/content/impact-cyber-crime-and-security-social-media

Stam, M. J. (2020). "How safe do you feel out alone online?". Fear of Crime and Cybercrime: a systematic literature review. *Malmö University: Faculty of Health and Society, Department of Criminology. .*

Sunday, O. (2020, June 12). *Newly-married man jailed for six months over internet fraud.*

Accessed from https://guardian.ng/news/newly-married-man-jailed-for-six-months-over-internet-fraud/

Sunday, O., & Ogune, M. (2020, January 29). *Mother, son jailed three years for $82,570 internet fraud*. Accessed from https://guardian.ng/news/mother-son-jailed-three-years-for-82570-internet-fraud/

TheCable. (2021, October 21). *Internet fraud: Eight Nigerians to face charges in US, risk 40 years imprisonment*. Accessed from https://www.thecable.ng/internet-fraud-eight-nigerians-to-face-charges-in-us-risk-40-years-imprisonment

The Guardian. (2022, April 8). *Court jails 3 over cybercrime in Ilorin*. Accessed from https://guardian.ng/news/court-jails-3-over-cybercrime-in-ilorin/

Theory, C. (2022, March 1). *Communication Theory*. Accessed from https://www.communicationtheory.org/technological-determinism/

ThisDayLive. (2021, April 2). *Bawa: EFCC Arrested 400 over Internet Fraud in Three Months*. Accessed from https://www.thisdaylive.com/index.php/2021/04/02/bawa-efcc-arrested-400-over-internet-fraud-in-three-months/

Uba, J. (2021, November 30). *Nigeria: The Legislative Framework For Cybercrime In Nigeria: Current Status, Issues And Recommendations*. Accessed from https://www.mondaq.com/nigeria/terrorism-homeland-security-defence/1136732/the-legislative-framework-for-cybercrime-in-nigeria-current-status-issues-and-recommendations

University Canada West, UCW. (2022). *How has social media emerged as a powerful communication medium?* Accessed from https://www.ucanwest.ca/blog/media-communication/how-has-social-media-emerged-as-a-powerful-communication-medium

United Nations Conference on Trade and Development, UNCTAD. (2021, December 14). *Cybercrime Legislation Worldwide*. Accessed from https://unctad.org/page/cybercrime-legislation-worldwide

United Nations Office on Drugs and Crime, UNODC. (2017). *Cybercrime*. Accessed from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html