Online Social Networks Misuse, Cyber-Crimes and Counter-Mechanisms in Nigeria

***Desmond Onyemechi Okocha**
Department of Mass Communication
Bingham University, Nigeria

Ozoemena Esther
Department of Mass Communication
Bingham University, Nigeria

Terhile Agaku
Department of Mass Communication
Bingham University, Nigeria

***Corresponding author: Okacha D. O. Email: desmonddoo@yahoo.com**

Abstract

This study provides a valuable understanding of how online social network has been used to perpetrate cyber-crimes and the counter mechanism to prevent such attack at the same time. The study was based on social learning theory. The research method adopted for this paper was qualitative research. In-depth interviews were used to collect primary data. A list of questions was prepared through Google Form as guidance for each interview session. Thirty (30) participants were chosen and divided into three batches (A, B, and C), using the convenient sampling approach. According to the findings of the study, criminals increasingly use online techniques such as stock spam e-mail and online extortion, cyber bullying, hacking of social media accounts, cyber theft, cyber harassment, cyber stalking, and cyber defamation. The study showed that cyber-crime cannot be eradicated and social media users ought to be careful and security conscious. It is a call for serious awareness by the government, the media, the Internet service providers, and users at large. Hence, the call to ensure security and privacy across all social media platforms is essential. Based on the findings of this study, it recommends that cyber education alongside other relevant domains should be taught from the elementary to the tertiary levels to avoid assaults and filter malware or suspected harmful code.

Keywords: Online Social Network (OSN), Cyber-crime, Social Media, Cybersecurity, Computer Crime

Introduction

Social media networks are platforms that allow people to engage and exchange multimedia material, via a website or an application, including text, music, video, photographs, graphs, and animations. Volume, diversity, velocity, validity, volatility, quality, and discovery are all cloud-based big data components.

According to the New Digital 2021 April Global Statshot Report, released in cooperation with Hootsuite and We Are Social, more than six out of every ten people on the globe now utilize the Internet. This has increased the penetration rate by more than 330 million and is expected to reach 5.3 billion by 2023. Moreover, it has become a fast means of both interpersonal and public communication. In Nigeria and the world at large, almost everyone in the community is connected to at least one social media platform. These have become part of human life as many individuals now rely heavily on information shared on social media. This new trend has broken boundaries and allowed people to become members of collaborative online networks, such as WhatsApp, Facebook, Instagram, Twitter, LinkedIn, YouTube, Pinterest, Snapchat, Quora, Tiktok, and WeChat which are just a few of the popular social media platforms. Due to the obvious larger user community and source of information available on social networks, many users have directly or indirectly exposed personal and intimate details about themselves. As a result, many corporate organizations, including banks, now rely on ICT and computer networks to perform basic and complex tasks. Everyone, including criminals, can now access the electronic market.

Computer security has become a global, academic, technological, social, and economic priority for all nations given that information security is a serious issue in information technology that poses a significant challenge. Of course, in both the private and public sectors, the Internet has become one of the rapidly growing mediums for business development (Schatz, Bashroush, and Wall, 2017). It is a widely used communication and information exchange medium. At the same time, the Internet is becoming a tool for numerous cyber-crimes as more organizations than ever before are conducting businesses online, according to the World Economic Forum's study Globalization 4.0.
Nigeria has lost nearly N5.5 trillion to *fraudulent* activities and cyber-crime in the last ten years, according to Bharat Soni (2021), a cyber-security awareness creator in Lagos, who also warned that cyber security threats and attacks might be the next pandemic.

Cyber-crime activities have rapidly evolved as a result of the necessity of computers in the current lifestyle, where everything from calculators to wristwatches, mobile phones, televisions, and nuclear power plants are run on computers. Cyber-crime has assumed dreadful implications which include hate crimes, hacking, cyber extortion, telemarketing and identity theft, credit card account thefts, drug trafficking, network spam, Internet fraud, network malware, cyber-bulling, and physical threats. While computer technology has improved the lives of many people, it has also created new opportunities for criminals (Bello, 2017). This study aims to provide a valuable understanding of how online social network has been used to perpetrate cyber-crimes and counters mechanism to prevent such attack at the same time.

Statement of the Problem

Cyber-crime is evolving at an alarming rate with new patterns developing all the time. Cybercriminals are becoming agile, utilizing new technology at rapid speed, adapting their assaults by using new approaches, and coordinating with one another in unprecedented ways. It appears that criminals utilize the infrastructure of online social networks (OSN) to carry out these activities. This research is carried out to provide a valuable understanding of how online social network has been misused to perpetrate cyber-crimes and counter mechanisms to prevent such attack at the same time.

Objectives of the Study

The research objectives are:

To identify how online social network has been compromised by their users.
To ascertain how cyber-crime has become a threat to online social networks.
To identify the determining factors for preventing cyber-crime.
To ascertain those responsible for creating awareness on social media about cyber-crimes

Research Questions

To guide the study, the following research questions are formulated:
How has the online social network been compromised?
To what extent has cyber-crime become a threat to online social networks?
What are the determining factors for preventing cyber-crime?
Who is responsible for raising awareness among social media users about cyber-crimes?

Theoretical Framework

This paper was anchored on Social Learning Theory by Albert Bandura (1977). Social learning theory states that observation and modeling play a significant role in how and why people learn. Reasons why individuals commit offenses is explained by a variety of criminological, sociological, and psychological perspectives. According to these hypotheses, social control, urbanization, learning, psychopathologies, class tension, and physiological deficits, all play a role in the genesis of cybercriminal conduct. This theory explains what motivates cybercriminals to engage in illicit activity (Rogers, 2006). This theory is pertinent to this study since it has indicated that these criminals are exposed to imitation and model definitions in their social context through seeing, learning, and mimicking.

Literature Review

The current outbreak of cyber-crime in Nigeria has been rather worrying and the detrimental impact on the country's socio-economic system is deeply concerning. Cyber-crime has evolved beyond traditional crimes as it poses a threat to the national security of all nations, especially technologically capable ones like the United States and Nigeria which is certainly not an exception.

Overview of Cyber-crime

The world is evolving and almost everything is dependent on the Internet, from traffic control, education, banking, healthcare, telephone to even wristwatches. This tremendous development has brought about changes in every aspect of human civilization, including crime. In March 2020, Europol published a warning about new methods through which cybercriminals profit from the epidemic and related lockdown measures. According to Europol's Internet Organized Crime Threat Assessment (October 2020),

"The worldwide COVID-19 epidemic produced an amplification of existing cyber-crime concerns," according to the report, and "due to the global COVID-19 outbreak," there has been an increase in fraud against enterprises. Law enforcement authorities in the United Kingdom utilized Twitter to promote public awareness about such concerns, allocating 57.2 percent of their posts to fraud schemes and 16.9% to cyber-crime issues (Nikolovska et al, 2020). Nigerians have morphed into cyber-creatures that spend much too much time on the Internet. In Nigeria, as the digital world grows, so does cyber-crime. In Nigeria, the term 'yahoo guys' is commonly used to refer to cybercriminals. Nigerian Cyber Laws arose from the necessity to address these seemingly uncontrollable phenomena.

According to a Center for Strategic Studies study, cyber-crime cost the world economy up to $600 billion in 2017, accounting for 0.8 percent of global GDP. As a global economic scourge, it ranks third only in government corruption and narcotics, and is equal to a 14% price on growth. In the United Kingdom, online fraud and cyber-crime account for half of all crimes (5.5 million offenses per year). The United Arab Emirates is thought to be the world's second-most targeted country, with an estimated annual cost of cyber-crime of $1.4 billion.

Panda Security (2018), on the other hand, categorizes cyber-crime into two types:

- Crimes that directly destroy computer networks and devices: malicious code, computer viruses, malware, and other such things are examples.
- Computer network or device-assisted crimes.

Various Cyber-crimes in Nigeria

Ways in which cyber-crimes are mostly carried out in Nigeria are discussed below:

Hacking: Hackers make use of operating system flaws and gaps to destroy data and steal sensitive information from the user's computer. It is usually done with the use of a backdoor application installed on a computer that allows for easy password hacking.

Cyber-Theft: The most prevalent and widely publicized cyber-crime is cyber-theft. It is the theft of electronic data using computers and communication devices. Computer hackers gain access to bank systems and transfer funds to their accounts. This is a major concern because huge sums of money can be stolen and unlawfully transferred. Another common occurrence is credit card fraud, most businesses and banks do not reveal that they have been victims of cyber theft.

Viruses and worms pose a significant threat to both ordinary users and businesses.

Email spam: This entails sending large quantities of email to promote and market items and websites.

Financial Fraud: This is referred to as "Phishing." It is the act of sending an e-mail to a user while posing as a reputable company in order to dupe the user into giving personal information that will be utilized for identity theft.

Cyberbullying is when someone uses technology such as the Internet, emails, or social networking sites to harass, threaten, shame, or target someone. Bullying, including cyberbullying, is prohibited.

Cyberstalking has been defined as a person who pursues or contacts a woman despite her evident indifference or who monitors a woman's usage of the Internet or electronic communication.

Cyber laundering is the electronic transfer of unlawfully obtained funds with the intent of concealing their source and, perhaps, their destination.

Cyber defamation is the use of computers or the Internet to spread slanderous information about another person.

Website Cloning: A current trend in cyber-crime is the appearance of bogus 'copy-cat' websites that prey on consumers who are inexperienced with the Internet or do not know the exact web URL of the actual organization they wish to visit.

Criminal activity videos: As smartphone and social media technology improves hand in hand, a growing number of criminals are broadcasting recordings of their crimes on social media.

E-commerce platform fraud: Such programs are used by fraudsters to deceive users into entering or submitting private financial information such as ATM numbers, UPI PINs, passwords, and so on.

Social media fraud: Fraudsters target major social media sites like Facebook and Instagram to create phony accounts. They perpetrate fraud by creating a similar fake account with the target profile's information and asking for immediate money transfers from their pals while claiming to be in a medical emergency.

Online job fraud: Cybercriminals use a variety of channels to market bogus job offers online, including phony websites.

The Essence of Cyber-Crime

The rampant use of social media means that Nigeria is not immune to the threat of online crime. Online crime is a sophisticated social phenomenon that poses a threat to society; it should be investigated and explored independently from other types of crime.

It has distinct qualities that set it apart from other sorts of crime, including the following:

Internet crime may be hidden.

it can also be multinational, and it employs a distant mode of perpetration with criminal organizations.

Online crime is strongly related to organized criminal organizations or online gangs, who are focused on more severe crimes as well as harmless "spam-sending" operations (Anderson, 2013). There are possibilities for not just clandestine contact between professional criminals and other people participating in unlawful operations, but also for a systematic settlement of large-scale criminal assignments.

Another issue with Internet crime, not only in Nigeria but also in other countries, is that, because professional and competent people perpetuate it, it draws the highly intelligent, who do not qualify as criminals in the traditional sense. On the 19th of February, 2022, Edo State Governor, Godwin Obaseki, observed that Internet fraudsters must be very brilliant to be able to dupe people and advised that their brilliance can be redirected to better causes. He further emphasized that the root cause should be addressed in the same manner as human trafficking.

Another reason Internet fraud continues to be rampant is that the family and friends of the fraudsters do not reprimand them. The youth who are in school take large amounts of money home to their parents, and though it is rarely acquired through legal means, they are celebrated for it. For some youth, cyber-crime creates an atmosphere that makes it appear as if it is a career because they have the impression that once you use a computer, you can make a career earning money online.

Social Media Misuse and Cyber-crime

Social media has not only changed the way things are done online, but it has also increased advocacy and citizens' participation in different aspects as almost everyone is an active social media user. In the past decade from 2010-2020, youth in Nigeria through social media moved causes and drastic measures were taken to address them by government and non-governmental organizations. Social media plays a huge role in cyber-crime and has contributed a lot to personal cyber dangers. The adoption of social media by personnel is overwhelming and so is the threat. Everyone, including criminals, can now access the electronic market and steal valuable data. This is made possible as we live in a world where we are eager to hand over our personal data.

There are two types of crime that are caused by cyber threats (McAlaney et al., 2018). Existing offenses are aided using Internet technology. Fraud is one example of a cyber-enabled crime. The initial assault vector is typically created through social media when the perpetrator searches for the victim's profile and approaches them. As a result, social media serves as an enabler of cyber-crime. However, because of the options provided by Internet technology, cyber-dependent crime exists. Cyber-enabled crime includes hacking and virus distribution, malicious URLs, Inference assaults, deanonymization attacks, link reconstruction attacks, click jacking, Sybil attacks, falsified profile attacks, and identity clone attacks. Because these crimes are regularly perpetrated and distributed over social media platforms, these channels serve as enablers for the motivated perpetrator and a suitable target's convergence (Saridakis et al., 2015).

Three individuals were apprehended in Lagos, according to INTERPOL's Cyber-crime Director in 2020. The offenders were charged with impersonating the personnel of an organization by generating phishing URLs, domains, and mass mailing operations. Agent Tesla, Loki, Spartan, and the noncore Remote Access Trojans were among the malware programs, spyware, and remote access tools delivered by these attacks. Before initiating frauds and siphoning cash, these applications were used to enter and monitor the systems of organizations and individuals. The gang was thought to have compromised government and business sector companies in over 150 countries by 2020.

Ramon Olorunwa Abbas, also known as Hushpuppi, a Nigerian social media personality, was arrested in Dubai in June 2020 on allegations of cyber-crime on two continents. According to CNN, the conspiracy involved wire fraud, money laundering, and monetary transactions on property obtained via illicit activities. However, his unlawful activities are entrenched in a society in which many young people regard fraud as the only way to generate money and regard fraudsters as hardworking individuals. As a result, numerous young men continue to effectively carry out illicit crimes by robbing trusting persons and institutions.

Among social media-related cyber-crime, pornographic content which does not reflect the moral values of society is distributed by social media users. As captured in Aliough (2019), one of the vehicles of pornographic content today is social media and this is done for financial purposes and ineffective regulation of the social media platforms. A vivid example of such was the popular ace singer, Tiwa Savage, who on the 8th of October 2021, revealed to American OAP, Angie Martinez of Power 105.1 Radio that she had been blackmailed by an unknown person who released an intimate video with her lover and asked for ransom which she refused to pay.

Popular platforms such as Facebook and Instagram recorded the highest number of cases with instances of defamation, posts of fake profiles, and vulgar comments on posts or messages. The number of such cases increased from 791 in 2020, to 1,518 in 2021 respectively.

Phishing is another popular "yahoo" crime in Nigeria. Phishing is an attack that involves sending a victim an email that appears to be from a genuine source, such as a bank. In phishing, the victim receives an email demanding personal information via a link to a phony website. The hacker will be able to access the victim's financial information after such information is given. According to Richards (2016), phishing emails sent by suspected hackers in Nigeria increased dramatically in 2015, spiking when the Central Bank of Nigeria (CBN) announced the Bank Verification Number (BVN) deadline. Unwary bank clients received phishing emails notifying them that their accounts had been compromised.

If Africa lost $3.5 billion to cyber-crime in 2017, Nigeria received $645 million, by far the largest share (Kshetri 2019). A year later, it was reported that cyber-attacks cost Nigeria $800 million (N288 billion) in 2018 (Azeez 2019). In general, according to a 2019 report, Nigeria has lost an average of N127 billion ($328,842,878 million) per year to cyber-crime in recent years (Ohwovoriole 2019). Cyber-crime is the most significant impediment to the widespread adoption of e-commerce and e-government in developing economies around the world. Governments can play a role in developing control mechanisms and enacting legislation to reduce cyber-crime. This will help to accelerate the spread of the Internet (Shalhoub & Al-Qasimi, 2010).

Counter Mechanisms

People utilize social media to communicate personal events, voice their opinions about socio-economic concerns, and engage with one another. Similarly, the criminal utilizes social media to commit a crime and uses technology to regulate, prevent, and investigate crime. People's perceptions of crime and victimization have shifted as a result of the increasing usage of social media in many aspects of life (Bartleby.com).

To prevent being a victim of cyber-crime, we must all take ownership of our online security and safety. This means adhering to safe online behaviors and being aware of how fraudsters gain personal information over the Internet. Here are some suggestions for preventing cyber-crime:

If your phone goes missing, disable your SIM card and reset the passwords to all your accounts.

Always set up a two-step verification password in all your social media account.

Be careful of email scams, protect your computer from cyber-attacks, and always maintain your antivirus and operating system up to date.

Don't write down or save the information required to access digital wallets/bank accounts on your phone.

Be cautious while purchasing online and avoid using third-party browser extensions, plug-ins, or add-ons, since they may track your activities and steal your personal information.

Safeguard your personal information and implement strategies to avoid exposure to inappropriate online content.

Do not reveal your password to any of your friends or coworkers, or even on any online form.

Avoid divulging information about your debit or credit card over these social media networks to avoid credit/debit card fraud.

Protect all your wireless access points with a secure password. Hackers look for open access points and take advantage of them to carry out nefarious actions. You may be more exposed to such abuse if you keep log recordings.

Use alphanumeric, special character, upper case, and lower-case combinations to create a strong password of at least 13 characters.

If you suspect your privacy has been violated online, notify (https://cyber-crime.gov.in) immediately.

It is easier to prevent these assaults when a company has a strong understanding of network security and an efficient incident response strategy. End-user protection, for example, secures information and protects against loss or theft while simultaneously screening PCs for harmful malware.

Methodology

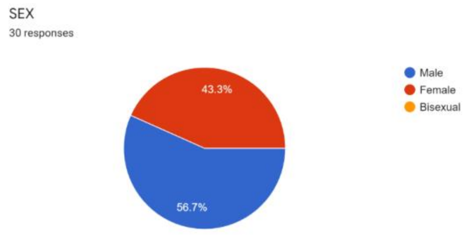
The research method adopted for this paper was qualitative research. Interview was the research technique while interview guides were used to collect primary data. Based on the research objectives, a list of questions was prepared through Google forms for each interview session concentrating on how online social network has been misused, cyber-crime, and counter mechanism. The convenient sampling method was used and 30 participants were selected and grouped into three Batches: A, B, and C. An online approach was adopted on different days to ascertain the participant's answers. The justification for selecting 30 participants is based on Creswell (1998) argument that in qualitative studies, sample size guidelines range between 20 and *30 participants*. Each interview session lasted for a period of 30 minutes via zoom, while the whole exercise lasted for 10 days (March 15-24, 2022). The data generated was analyzed qualitatively.

In-depth interviews are a qualitative data collection method that allows for the gathering of information about the interviewees' behavior, attitude and perception. It also involves direct or one-on-one engagement with individual participants or over the phone in some cases.

Data Presentation and Analysis

The data derived from the responses gathered from the interview guide are presented and analyzed below:

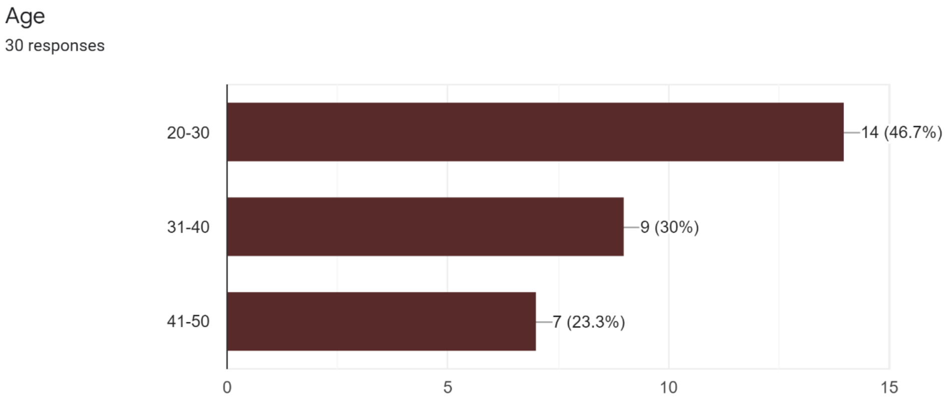
Figure1: Sex of the Participants



Source: Field survey, 2022

Figure 1 shows the distribution of participants on demographic information with 11 of the participants being female and 19 participants were male. This shows that there were no bisexual participants.

Figure 2: Age of Participants



Source: Field survey, 2022.

It was discovered from figure 2 that 14 of the participants are of the age bracket 20-30 years, 9 of the participants fall within the age bracket 31-40 years, 7 of the participants are of the age bracket 41-50 years

Question 1: Participants on social media usage on a scale of 0-10

The activeness of the participants on social media on a scale of 0-10 indicates that 3 of the participants ticked 0-2 to indicate their frequency on social media. 7 ticked 3-5, which indicated how frequent they are on social media while 20 ticked 6-10 which clearly stated that they are very frequent on social media.

This implies that most of the participants in this study on the 6-10 scale indicate that they are very frequent and active on social media.

One of the participants in Group A stated:

That social media serves as a platform for global social engagement. People use social media to express themselves, share their ideas and habits, engage with friends, and meet new people. The larger user base of social media sites reflects their popularity.

Question 2: Most frequently used social media sites

ALL the participants affirmed that they are very active social media users of Facebook, Twitter, WhatsApp, Instagram, TikTok, LinkedIn, and YouTube.

It revealed that social media platforms have become an important part of people's lives as they are highly reliant on them because they aid in the formation of social interactions and the formation of strong online communities.

Question 3: How much the users know about cyber-crime

It was revealed through the interview that the participants are quite knowledgeable of the term cybercrime; only three persons out of the thirty participants interviewed stated that they are not aware of the term.

The participants in Group C said:

Computer crime and abuse are high. Many online social media users are victims perpetrated by those who take advantage of anonymity to their identities to harm users both in virtual and in the real-world daily.

Another, in Group B, disclosed that:

The use of a computer as an instrument to further illegal ends, such as fraud, trafficking in child pornography and intellectual property, stealing identities, or invading one's privacy, is also called cyber-crime.

Question 4: The online social network has been compromised by their users

25 participants blamed online social networks for making it easy to commit various types of cyber-crimes such as stealing and manipulating users' private information. Theft of an Internet user's vital information and data is becoming more common. Criminals are increasingly using Internet tactics such as sending mass spam e-mails, online extortion, cyberbullying, hacking of social media accounts, cyber theft, cyber harassment cyberstalking, cyber defamation, and many more.

Sadly, nine of the participants revealed that they have also been victims of some of these online crimes, especially cyberbullying and extortion.

Another participant in Group A also stated:

My social media account was hacked recently and used to extort money from my friends, claiming that I was seriously ill.

Question 5: Cyber-crime threats to online social networks

This question was an open-ended question guide where the participants shared their views that cyber-crime has become a big threat to online social networks and the economy at large. One of the participants added that it has nullified the original purpose of the social network and all the users are at serious risk. The participants also stated that economic and technology factors contribute to cyber-crimes while only one person mentioned societal factor. This is to say that Internet criminals have taken advantage of technological advancement; hence, this has become a threat to the world at large and needs to be urgently addressed.

Question 6: Raising awareness among social media users on cybercrimes

Among the interviewees, 15 stated that the media, the social media users and the service providers play a major role in creating awareness. To this question, 15 mentioned that it is the government's responsibility to create cybercrime awareness.

A participant in Group B boldly stated that:

The use of social media platforms by billions of people across the world has enticed hackers to transmit dangerous code, spam users' inboxes, and even try to undermine users' innate faith in these platforms on the relationship and its network.

At the end of the interview session, it was agreed by all the participants that:

It is a call for serious awareness by the government, the media, the Internet service providers, and users at large. Hence, maintaining security and privacy on all social media platforms is essential. Social big data may be utilized in real-time to prevent crime or offline to investigate it.

Question 7: Prevention of cyber-crimes

The participants listed different preventive methods such as raising more awareness and putting measures in place to prevent cyber-crime by setting up a two-step verification that is strong enough to prevent crime.

One of the participants in Group C said that.

Cyber-crime cannot be eradicated as there is no regulatory body for social media platforms yet. This should be considered in order to curb cyber bullying and the users are also enjoined to be careful and security conscious.

This implies that increase in individual awareness will have a stronger influence on the situation. Thus, developers should ensure stringent antivirus and the creation and availability of anti-malware on apps and websites developed.

Discussion of Findings

This study aims to provide a valuable understanding of how online social network has been misused for cyber-crimes and the counter mechanism to prevent cyberattacks. It is important to mention that social media has evolved into a more efficient instrument for (re)producing and (re)distributing information, and the popularity of social media platforms is mirrored in their larger user base. A total of 30 participants whose views were gathered have smartphones and other digital gadgets which gives them access to connect with others and socialize actively on all social media websites such as WhatsApp, Facebook, TikTok, LinkedIn, and YouTube, Instagram, email, and many others. In their study on the use of ICT tools, Santas and Idowu (2018) agree with the preceding views.

The study sought to identify how online social network has been compromised by their users. It was also discovered that criminals have increasingly employed online strategies such as stock spam e-mail, online extortion, cyber bullying, hacking of social media accounts, cyber theft, cyber harassment cyber stalking, cyber defamation, and many more. Sadly, some of the interviewees revealed that they have also been victims of some of these online crimes. This aligns with (Kawasaki & Fitzpatrick, 2014) argument that while the proliferation of crime on social media has brought numerous concerns, including uncertainties about its efficacy, it has not lessened its social benefit.

The study was also conducted to ascertain how cyber-crime has become a threat to online social networks. In response to this objective, data evidence revealed that cyber-crime has become a threat to online social networks. It has been revealed that the factors that contribute to cyber-crimes are economic factors, technology factors, and societal factors.

Because of its widespread usage, the Internet has altered work and leisure activities. This implies that cybercrime has become a threat to online social networks because of economic, technological and societal factors. This finding agrees with Kemp et al. (2020) argument that criminals may dedicate more time to online crimes, such as cyber-enabled fraud. Indeed, studies have indicated that dramatic rises in "cyber" fraud are driving overall increases in fraud.

The study was also carried out to identify the factors for preventing cybercrime. Data evidence revealed that the determining factors for preventing cybercrime includes raising more awareness and putting measures in place to prevent cyber-crime, setting up a two-step verification that is strong enough to help prevent crime. One of the participants stated boldly that cybercrime cannot be prevented but enjoined users to be security conscious and careful. This denotes that awareness from individual to individual will have a stronger influence on the situation. U.K law enforcement agencies utilized Twitter to promote public awareness about such concerns and allocated 57.2 percent of their posts to fraud schemes and 16.9 percent to cybercrime issues. This implies that the factors for preventing cybercrime range from creating awareness as well as taking measures to prevent cyber-crime to setting up a two-step verification with a view to preventing crime. This finding agrees with Rogers (2006) submission that the social learning theory explains what motivates cybercriminals to engage in illicit activity.

The study also sought to investigate those who are responsible for creating awareness on social media about cyber-crimes. Data evidence revealed that the government, the media, and users cannot do it alone as affirmed by some participants. It is a call for serious awareness by the government, the media, the Internet service providers, and users at large. Hence, it is critical to ensure security and privacy on all social media sites. The implication is that creating awareness on social media about cybercrime is the duty of all and sundry. This finding is supported by Saridakis et al. 2015) position that crimes are regularly perpetrated and distributed over social media platforms, these channels serve as enablers for the motivated perpetrator and a suitable target's convergence.

Conclusion

The study concludes that cybercrime poses significant danger to online social networks. It is also important to note that whenever technology advances, cyber-crime increases. Cybercriminals are more interested in online social networks since a variety of users lack social networking awareness. We can reduce the threat of cyber-attack or cyber-crime by being aware and conscious while using social media platforms.

Recommendations

Having established the findings of this research, the recommendations are thus:

When using the Internet, it is advisable not to disclose personal identification number (PIN), bank account information or e-mail address to strangers since systems are vulnerable.

Cyber education should be taught from the primary level to the tertiary level by institutions of learning.

To avoid assaults and filter malware or suspected harmful programs, financial institutions and social media users should utilize firewalls properly and consistently.

Internet service providers should develop soft wares that will protect social media users against cybercrimes.

References

Auwal, M.A. & Abdullahi, A. (2018). Conceptualizing the access, control, and intricacies ofsocial media in Nigeria. *Nasarawa Journal of Multimedia and Communication Studies 1*(2).

Asad, M. and Ghulam, S. (2018). Social media and cyber-crimes in Pakistan: Facts, propaganda, awareness, and legislation. *Global Political Review 3*(2), 84-97. DOI: 10.31703/gpr.2018(III-II).09

Bartleby.com. Essay about social media is a source for criminals and law enforcement https://www.bartleby.com/essay/Social-Media-is-a-Source-for-CriiminalPKJBZXUSVC

Burruss, G. W., Bossler, A. M. and Holt, T. J. (2012). Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy. *Crime and Delinquency,* 59(5), 1157-1184. DOI: 10.1177/0011128712437915

Bello, T. (2017). Anatomy of cybercrime in Nigeria: The legal chronicle. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3055743

Britannica.com "computer security | Definition & Facts | Britannica". www.britannica.com. Retrieved August 8, 2022

Benson, V. (2017). The state of global cyber security: highlights and key findings. L T Inc, UK DOI: 10.13140/RG.2.2.22825.49761

Cohen, L. E., Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589
Google Scholar.

Collins, J. D., Sainato, V. A. and Khey, D. N. (2011). Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *Cybercrime Journal5*(1), pp 794-810[Online] Available from<HTTP://www.cyber-rimejournal.com/collinsetal2011ijcc.pdf>

Patel, M. (2017). Cyber security for social networking sites: Issues, challenges and solutions. International Journal for Research in Applied Science and Engineering Technology. **file:///C:/Users/ESOFT/Downloads/00001.pdf**

Johns, E. (2021). Cyber security breaches survey 2021. *Department for Digital, Culture, Media,*
and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf
Google Scholar

Europol. (2020a). Internet organized crime threat assessment (IOCTA) https://www.europol.europa.eu/sites/default/files/documents/Internet_organised_crime_threat_assessment_iocta_2020.pdfGoogle Scholar

Hinduja, Sameer and Kooi, Brandon. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. Security Journal, 26(4), 383-402

https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cyber-crime-phishing-threat-needs-urgent-government-action economy/#:~:text=A%20report%20by%20the%20Center,a%2014%25%20tax%20on%20growth

International conference on information security & privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Ibikunle Frank and Eweniyi Odunayo, (2013), “Approach to cyber security issues in Nigeria: challenges and solution” vol. 1, no.1,

Igba, D. I.; Elizabeth, C. I.; and Aja, S. N. (2018). examine cyber-crime among university undergraduates: implications on their academic achievement. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2 (2018) pp. 1144-1154 © Research India Publications.

Interpol (2020). Cyber-crime: COVID-19 impact.https://www.interpol.int/content/download/15526/file/COVID19%20Cyber-crime%20Analysis%20Report-%20August%202020.pdf. Accessed 09/10/2020Google Scholar

Muhammad, A. Y. (2021). Journal of intelligence and cyber securityhttps://www.researchgate.net/publication/355773516_Cybersecurity_and_Cyber-crime_in_Nigeria_The_Implications_on_National_Security_and_Digital_Economy

Moga, E and Salihu, A G. (P) (2021). A historical assessment of cyber-crime in Nigeria: implication for schools and national development. *9*(9) pp: 84-94

Schatz, D., Bashroush, R. and Wall, J. (2017).Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law. 12*(2). ISSN 1558-7215.

SIrshad, I. and Soomro, T. R. (2018). Identity theft and social media. *International Journal of Computer Science and Network Security*, *18*(1), pp. 43–55.

Tennakoon, H., Saridakis, G. and Mohammed, A-M. (2018). Child online safety and parental intervention: A study of Sri Lankan internet users. Information Technology & People, 31:770-790.

Uba, J. (2021). Cyber-crimes and cyber laws In Nigeria: All you need to know. https://www.mondaq.com/nigeria/security/1088292/cyber-crimes-and-cyber-laws-in-nigeria-all-you-need-to-know

Uche, I. (2021). Nigeria’s growing social networking sites. https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cyber-crime-phishing-threat-needs-urgent-government-action-economy/