Vulnerability of Cybercrime Victimization: Causes, Pattern and Solutions in Gombe Metropolis

[1]Anslem Ali, [2]Ahmed Tanimu Mahmoud, [2]Adeyinka T. Yusuf, [2]Halliru Tijjani
[1]The Nigeria Police Force, Gombe State Command
[2]Department Criminology and Security Studies, National Open University of Nigeria (NOUN) Abuja
Corresponding Author: Anslem A. keshione71@yahoo.com,

Abstract
This study examines the vulnerability to cybercrime victimization in Gombe Metropolis, focusing on its causes, patterns, and solutions. The research employs a cross-sectional survey design to capture the phenomenon at a specific point in time. A total of 200 valid responses were analyzed, gathered from residents, businesses, and organizations vulnerable to cybercrime. Data collection utilized a five-point Likert scale questionnaire, and sampling techniques included purposive selection of the study area and convenience sampling across different demographic groups. Analysis was conducted using SPSS version 23, with zero-order correlation testing the relationship between cyber security awareness and vulnerability, and one-way ANOVA assessing the impact of awareness on vulnerability levels. The findings revealed a paradoxical relationship: as awareness of cybercrime increased, vulnerability also rose, potentially due to increased reliance on digital platforms without corresponding protective behaviors. This study suggests that mere awareness is insufficient to mitigate cybercrime risks and highlights the need for a comprehensive approach to cyber security, including behavioral change, effective protective measures, and policy interventions. The significant influence of awareness on vulnerability ($F(3,197) = 4.189$, $p < 0.05$) supports existing literature on the heterogeneity of cyber security postures. Recommendations include strengthening cyber security infrastructure, launching awareness campaigns, providing specialized law enforcement training, fostering collaboration, and enacting robust cybercrime legislation. The study contributes to the understanding of cybercrime dynamics and calls for holistic strategies to reduce cyber threats in Gombe Metropolis.

Keywords: *Cybercrime, Cyber security, Metropolis, Vulnerability, Victimization*

Introduction

The evolution of the Internet amidst a rapidly growing global economy has created a completely new environment in which traditional crime prospers. Equally, the convergence of computing and communication has changed the way we live, communicate and commit crimes (Muktar, 2018). In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gains in productivity, efficiency, and communication they also create a loophole that may destroy an organization. This is evident in the way and manner some criminal elements carry out their operations using internet technologically related tools to cause mayhem in the smooth running of an individual(s) or organizational activities like communication, conducting business transactions, health care management, education delivery, environmental monitoring, etc. This heavy reliance on technology has made humans susceptible to various kinds of threats associated with the wrongful use of computer technology.

Several writers and commentators have argued that full-scale organized cybercrime is fast emerging (Lusthans, 2013). Systems that people rely upon, from bank to air defense radar, are accessible from cyberspace and can be quickly taken over and knocked out without first defeating a country's traditional defenses (Clarke &Knake, 2010). The growth of information

technology and computer connectivity creates space for criminals to exploit security vulnerabilities in cyberspace (Kigerl, 2012). Unfortunately, several functionalities of modern-day web browsers are not vulnerability-proof (Agbefu et al, 2013), thus exposing the average internet user to cybercrime victimization. With mobile telephony access made pretty easier over the past half a decade in Nigeria through the offering of internet services by virtually all Global System for Mobile Communication (GSM) service providers in Nigeria, the internet has pervaded the lives of many adult Nigerians (Philip, Emmanuel, Igbo, &Uzoma, 2013).

A secure digital environment is a subject of great importance in the current reality in the information society and the new economy that set the course of the culture, economy, and progress of the world today. Daily traffic on the Internet increases considerably, and thousands of users access various websites to consume some product or service of the many that digital companies currently offer, however, the digital ecosystem is highly vulnerable to attacks by digital criminals which endanger the safety of users, who may be damaged in their property or their person. Therefore, each nation needs to have an up-to-date legal system capable of effectively protecting users against any criminal behavior typical of this technological environment (Doris, 2017).

However, although Nigeria is one of the top cybercrime-prone countries, not many studies have examined the dynamics of the vulnerability of cybercrime victimization in Nigeria which leads the current study to find how vulnerable the victims of cybercrime are which will help the researcher to find out the reasonable measure to reduce the menace.

Statement of the Problem

Gombe metropolis is witnessing an alarming increase in cybercrime victimization, posing significant threats to individuals and organizations (VON, 2023). This escalating vulnerability raises concerns about the underlying causes, intricate patterns, and the absence of tailored solutions to address this pressing issue. The lack of comprehensive understanding of the factors contributing to vulnerability, coupled with a dearth of insight into the specific patterns of cybercrime in Gombe metropolis, hinders the development of effective preventive measures. Consequently, this research aims to delve into the multifaceted aspects of cybercrime victimization exploring the root causes, discerning patterns and proposing viable solutions to safeguard the digital landscape in Gombe metropolis.

Research Question

This research has the following research questions:-

1. What are the primary causes of vulnerability of cybercrime victimization in Gombe metropolis?
2. What patterns characterize cybercrime victimization in Gombe metropolis?
3. What potentials solutions can be identified to mitigate the vulnerability of cybercrime victimization in Gombe metropolis?

Objectives of the Study

1. To investigate the root causes contributing to the vulnerability of individuals and organizations in Gombe metropolis.
2. To examine and analyze the patterns and trends of targeted of targeted demographics, methods, employed and types of cybercrime prevalent in Gombe metropolis.
3. To propose effective solution to enhance cyber security measures, raise awareness and reduce the vulnerability of residents and organizations to cybercrime in Gombe metropolis.

Hypothesis

Ho: There is a significant relationship between the level of cyber security awareness and the vulnerability of individuals and organizations to cybercrime victimization in Gombe metropolis.

Hi: People who not aware of cybercrime would significantly be more vulnerable than people who are aware of effective cyber security measure to result cybercrime victimization in Gombe metropolis

Literature Review

The term online fraud, also known as internet fraud, encompasses a variety of deceptive practices that utilize internet services like chat rooms, email, online forums, or websites to carry out fraudulent activities targeting potential victims. These fraudulent activities typically aim to trick individuals into divulging personal information or parting with their money through methods like credit card theft, money transfers, or the disclosure of sensitive account information. Online fraud can lead to financial or non-financial losses for those who fall prey to these schemes (Singh, 2014).

In essence, online fraud can be defined as the act of using internet resources to engage in dubious transactions with the intention of deceiving or defrauding individuals, organizations, or even governments (Moore, 2014). It occurs when individuals respond to deceptive online solicitations, notifications, offers, or requests by providing funds or personal information, ultimately resulting in their suffering financial or other types of losses (Cross, Smith & Richards, 2014). Although the tactics employed by online fraudsters may vary, their ultimate goal is consistent: to acquire something valuable, whether it's personal information or money, through misleading and dishonest means (Cross, Smith & Richards, 2014).

The shift of criminal activities like fraud from the physical world to the online environment has been proposed as a contributing factor to the decrease in traditional offline crimes (Williams, 2016). Online fraud can manifest in different forms, such as romance fraud, deceptive sales of products and services, fraudulent investment schemes, inheritance scams, work-from-home schemes (often used for money laundering), or lottery fraud involving fake prize drawings or sweepstakes (Button et al., 2014; Button, Lewis & Tapley, 2009; Chang, 2008; Cross, Smith & Richards, 2014). These fraudulent activities are often accompanied by technological methods like malware, phishing, vishing (voice phishing), or skimming, which aim to deceive users into revealing personal information, making financial transfers, or electronically acquiring their personal data without their knowledge (Button et al., 2014; Chang, 2008; Cross, Smith & Richards, 2014). Many victims only become aware of their victimization when they are alerted by banks, credit agencies, debt collectors, or law enforcement.

According to Eze-Michael (2021), it's important to distinguish online fraud, also known as Internet Fraud, from cybercrime. Internet Fraud is considered a subset of cybercrime, with cybercrime encompassing various other types of illicit activities, including cyber stalking, cyberbullying, online trafficking, child pornography, cyber terrorism etc. On the other hand, Internet Fraud comes in various forms, such as phishing, ATM fraud, online counterfeit shopping, scareware or malware, Business Email Compromise (BEC), data breaches, Email Account Compromise (EAC), ransomware, identity theft, lottery fraud, social media fraud, and matrimonial dating fraud. Internet fraud and computer fraud are often used interchangeably to describe the same concept.

Online fraud has evolved into a modern phenomenon that enables perpetrators to reach homes and offices, cross borders, and easily access victims, particularly given the internet's pivotal role in providing financial and banking services. Cybercriminals continually devise new methods and exploit vulnerabilities to carry out their activities. As a result, information security companies, banks, and financial institutions have established specialized technology departments to safeguard customers and secure online financial transactions. Experts in the field regularly discover new tools used in online fraud, ranging from deceptive email messages to everyday online conversations and various communication methods. The internet has become an unpredictable risk, with hackers constantly on the lookout for their next target (Rusch, 1999). The rise in cybercrime has introduced a new set of criminal activities that differ from traditional crimes. Perpetrators can commit cybercrimes from the comfort of their own homes, making entry into the online world

effortless. These crimes go beyond network breaches and information theft, extending to include moral offenses like extortion, kidnapping, and even murder (McGuire & Dowling, 2013).
Advance fee fraud stands out as one of the prevalent techniques used by individuals seeking to defraud victims of online fraud. In 2017, Australian Competition and Consumer Commission (ACCC) reported that the most common types of scams leading to financial losses were upfront payment and advance fee frauds, along with other purchasing and selling scams (ACCC, 2018). Victims often fall for advance fee fraud when they respond to emails promising substantial benefits or rewards in exchange for a relatively small upfront payment. Regrettably, these promised benefits never materialize.

While some online frauds aim to extract money directly from their victims, others are designed to obtain personal information that can subsequently be used to acquire money. Phishing is a prime example of the latter type of fraud. In phishing schemes, fraudsters create convincing replicas of legitimate websites or emails to deceive unsuspecting individuals into providing their personal information, either through email or by filling out counterfeit online payment forms. To alleviate any doubts the victim might have regarding the authenticity of the fraudulent communication, the fraudsters may produce false documents or construct imitation websites as supposed 'proof' of its legitimacy. Studies have revealed that one of the primary reasons people respond to fraudulent invitations is because they appear to come from reputable and legitimate sources (Button, McNaughton, Kerr & Owen, 2014; Dhamija, Tygar& Hearst, 2006).

Theoretical Framework:
Routine Activity Theory
The Routine Activity Theory was proposed by Cohen and Felson 1979 in (Miller, 2006). They contended that for a crime to take place three requirements needed to be present; a motivated offender, a suitable target, and absence of capable guardians.The theory argues that crime is normal and depends on the opportunities available. If a target is not protected enough, and if the reward is worth it, crime will happen. Crime does not need hardened offenders, super-predators, convicted felons or wicked people. Crime just needs an opportunity. It states that for a crime to occur, three elements must be present at the same time and in the same space when any crime is committed, thus:

i. A suitable target is available
ii. There is the lack of a suitable guardian to prevent the crime from happening
iii. A likely and motivated offender is present.

However, with an increasing internet penetration especially in developing countries, the number of targets and offenders increases daily. It is difficult to estimate how many users of the internet are using it for illegal activities (UNODC, 2013).

The Theory of Technology-Enabled Crime
The key insight into the theory is that, it combines several categories of criminological theories to help society better understand why crimes co-evolved with computer and telecommunications technologies to become among the most complex and difficult forms of crime to prevent, investigate and control. McQuade (2006) reveals that understanding and maintaining relatively complex crime is initially quite difficult, and there is continual competition between the criminals and law enforcement for technological advantage. As criminals do something new and innovative, law enforcement must catch up in order to avert, control, deter, and prevent new forms of crime. McQuade argues that, technology enable crime theory encompasses:

i. Crimes committed directly against computers and computer systems.
ii. Activities which fall under this category are often referred to as high tech crime, computer crimes or cybercrimes.
iii. The use of technology to commit or facilitate the commission of traditional crimes.
iv. Crimes such as fraud, scams, and harassment can be facilitated using technology which brings unique challenges to old crimes.

The theory provides a framework for understanding all forms of criminality and especially those that are evolving with computing and telecommunications technology inventions and innovations. The theory is appropriate for understanding contemporary threats posed by emerging forms of cybercrime, transnational crime and terrorism networks that defy traditional methods criminal justice and security measures for preventing and controlling crime.

It is therefore relevant to this study because it provide us insight understanding of the new tools and techniques use by cyber- criminals; that is, a shift from the simple crime committed using simple tools to complex crime committed using complex tools. It also helps in understanding the new forms of deviance, social abuse or crime committed through innovative use of technology. Similarly, the theory reveals that people become victims of cybercrime because of the increasing advancement of technology where some individuals take advantage of it commit different forms of crime.

Methodology

The study adopted the cross-sectional survey design. Cross-sectional design according to Singh, M.S (2016) refers to a one-time study or measurement of an exposure or outcome of a phenomenon under study. This design best fits the study because the research was set out to assess the vulnerability of cybercrime victimization: causes, pattern and solutions in Gombe metropolis. Cross-sectional descriptive research is focused on observing, documenting, and describing the situation or occurrence of phenomena. This was done through the administration of five points Linkert scale questionnaire to the victims of cybercrime in Gombe metropolis in other to assess how vulnerable they are before becoming victims of cybercrime.

The population of the study comprised of resident of Gombe metropolis, including individuals, business and organizations directly impacted by or vulnerable to cybercrime.

Considering the diverse nature of Gombe metropolis, a total of 208 participants were drawn which deemed sufficient to achieve reliable result. This was determined based on a confident level of 95% and margin error of 5%.

Purposive sampling technique was used to select Gombe metropolis in Gombe State, Nigeria. Convenience sampling technique was used to sample participants across different age groups, professions and organizational types. This help greatly in understanding of cybercrime vulnerability among various segments of the population.

The issue of informed consent was clearly observed by collecting data from participants who willingly indicated their interest to participate in the study. They were told that participation in the study is voluntary and that they can decline to response to the questionnaires at any point in time. Also, there was no inducement or monetary reward for participation in the study. The questionnaire took 15 minutes on the average to fill. A total of 208 questionnaires were distributed, two participants refused to hand in the questionnaire while 206 were retrieved (i.e., 99% response rate). However, six questionnaires were half-filled and were removed left with 200 questionnaires that were used for the final analysis.

Data collected for the study were analyzed using the Statistical Package for Social Science (SPSS) version 23 tool to analyze the responses obtained from questionnaires administered. Hypothesis one was tested with zero-order correlation, while Hypothesis two was tested using One-way ANOVA showing the level of awareness status of vulnerability of cybercrime victimization in Gombe metropolis.

Results

Ho: There is significant relationship between the level of cyber security awareness and the vulnerability of individuals and organizations to cybercrime victimization in Gombe metropolis.

Table 1: Zero-order Correlation among Cybercrime victimization, vulnerability of individuals and organizations to cybercrime victimization in Gombe metropolis.

S/N	Variables	1	2	3	4
1.	Cyber secrity awareness	-	-.362**	.415**	.291**
2.	Vulnerability of individuals and organization		-	-.149**	-.311**
3.	Cybercrime victimization			-	-.612**

** Correlation is at .05

Result from Table 1 revealed that cybercrime awareness had significant positive relationship with vulnerability of individuals and organizations (r =.415, p <.05) and patternsof cybercrime victimization(r =.291, p <.05) but inversely correlated with solutions (r =-.362, p <.05). The stated hypothesis is confirmed.

Hi: People who not aware of cybercrime would significantly be more vulnerable than people who are aware of effective cyber security measure to result cybercrime victimization in Gombe metropolis

Table 2: One-way ANOVA showing the level of awareness status of vulnerability of cybercrime victimization in Gombe metropolis.

Source	SS	Df	MS	F	p
Between groups	5744.129	3	152.181	4.189	<.05
Within groups	113401.221	197	187.675		
Total	121052.164	200			

Table 2 presents result the level of awareness status of vulnerability of cybercrime victimization in Gombe metropolis. The result revealed that level of awareness had a significant influence on vulnerability of cybercrime victimization [$F(3,197) = 4.189, p < .05$].

Discussion of Findings

This study investigated the vulnerability of cybercrime victimization: causes, pattern and solutions in Gombe metropolis. From the above findings is revealed that cybercrime awareness had significant positive relationship with vulnerability of individuals and organizations and patterns of cybercrime victimization but inversely correlated with patterns and solutions among people living in Gombe metropolis.This finding suggests that as awareness increases, there is a corresponding increase in vulnerability. This paradoxical relationship might be attributed to several factors, such as an increased reliance on digital platforms as individuals become more aware, potentially exposing them to a higher risk of cyber threats. It may indicate that, while awareness can empower individuals and organizations to recognize potential threats, it might not necessarily translate into effective protective behaviors or risk mitigation strategies.
Table 2, the results of the one-way ANOVA provides further depth to the understanding of the relationship between awareness and vulnerability. The findings reveals that the significant influence of awareness on vulnerability ($F(3,197) = 4.189$, $p < 0.05$) emphasizes that the varying levels of awareness among individuals and organizations in Gombe metropolis are associated with differences in vulnerability to cybercrime victimization. This aligns with broader cyber security literature that acknowledges the heterogeneity in the cyber security postures of entities based on their awareness levels.

In relating these findings to existing scholarly literature, it is important to consider research that discusses the multifaceted nature of cyber security awareness. Studies emphasizing the need for a holistic approach, encompassing not just awareness but also understanding, implementation, and adaptability, align with the unexpected results observed in this study (Anderson & Moore, 2020). Moreover, research exploring the psychological aspects of cyber security decision-making may shed light on the inverse correlation with perceived solutions.

Summary

This study focuses on Gombe metropolis, Nigeria, where cybercrime victimization is on the rise, raising concerns about the causes, patterns, and lack of tailored solutions. The research questions explore the primary causes, patterns, and potential solutions to cybercrime vulnerability. Using a mixed-methods approach, data was collected from 200 participants through a cross-sectional survey design. Findings reveal a

paradoxical relationship: as awareness increases, vulnerability also rises. The one-way ANOVA shows significant differences in vulnerability levels based on awareness. These results suggest a need for a more nuanced understanding of cyber security awareness, moving beyond knowledge to effective protective behaviors. The study contributes to the literature by emphasizing the multifaceted nature of cyber security awareness and the importance of holistic approaches to address cyber threats effectively.

Conclusion

The findings from this study contribute to the ongoing scholarly discussion on the relationship between cyber security awareness and vulnerability. The unexpected results highlight the need for a more nuanced understanding of how awareness translates into protective behaviors and the perceived effectiveness of implemented solutions. Future research should explore the contextual factors influencing these relationships to inform more targeted and effective cyber security education and intervention strategies.

Recommendations

The research recommends the following:

1. Government should strengthening cyber security infrastructure in Gombe Metropolis is paramount to mitigate the vulnerability to cybercrime. Invest in advanced technologies, regular security audits, and the implementation of robust cyber security protocols to safeguard individuals, businesses, and governmental entities from cyber threats.
2. Government and NGOs should launch comprehensive awareness campaigns to educate the public, businesses, and government officials in Gombe Metropolis about the risks associated with cybercrime.
3. Government should provide specialized training for law enforcement agencies in Gombe Metropolis to equip them with the necessary skills and knowledge to combat cybercrime effectively.
4. Public, government and NGOs should encourage collaboration and information sharing between law enforcement agencies, businesses, and other stakeholders to create a united front against cyber threats.
5. The public should advocate for and enact robust cybercrime legislation that addresses the unique challenges posed by cyber threats and ensure that the legal framework is equipped to prosecute cybercriminals effectively and acts as a deterrent to potential offenders.

References

Adeniran, A. I. (2008). The Internet and Emergence of Yahoo-boys Sub-Culture in Nigeria.*International Journal of Cyber Criminology*, 2(2), 368–381.

Adeniran, A. (2011). Café culture and heresy of yahooboyism in Nigeria. In K. Jaishankar, (Ed.), *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. 3-12). Boca Raton, FL, USA: CRC Press.

Adomi, E (2016), 'Overnight Internet Browsing Among Cybercafe Users in Abraka, Nigeria', Advanced Free Fraud in West Africa, pp 33-34. Nigeria: EFCC

Australian Competition and Consumer Commission (ACCC) 2018. *Targeting scams: Report of the ACCC on scams activity in 2017.* Canberra: ACCC

Afolabi, M. B. &Esoso, A. J. (2021) Cybercrime Ordeal in Nigeria Security Firmament. *Sapientia Global Journal of Arts, Humanities and Development Studies* (SGOJAHDS), Vol.4 No.1; p.g. 257 – 268; ISSN: 2695- 2319 (Print); ISSN: 2695-2327 (Online)

Agbefu, R. E., Hori, Y., & Sakurai, K. (2013).Domain information blacklisting method for the detection of malicious web pages.*International Journal of Cyber Security and Digital Forensic*, 2(2), 36 -47.

Akano, D. (2016). Switzerland to return S380m Abacha loot. Daily Independent, March, are Younger Internet Users. In K. Jaishankar (Ed.). *Interpersonal Criminology: Revisiting Interpersonal Crimes and Victimization*. pp. 203 – 214

Anderson, R., & Moore, T. (2020).Cybercrime and Its Impact on Individuals,

Organizations, and Society.In*Handbook of Research on Cyber Crime and Information Privacy* (pp. 1-16).

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., &Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior, and Social Networking*, 21(2), 84–90.

Bijik H. A., David L. F., &Makinde, J. (2012) "ARPN Journal of Science and Technology::Cybercrime in Nigeria: *Causes, Effects and the Way Out*," ARPN J. Sci. Technol., vol. 2, no. 7, 2012.

Bhandari, P. (2020). What is qualitative research? Methods and examples.Scribbr. Retrieved from https://www.scribbr.com/methodology/qualitative-research

Button, M.; McNaughton Nicholls, C.; Kerr, J. & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54. https://doi.org/10.1057/sj.2012.11

Catherine D. Marcum and George E. Higgins Cybercrime in, Krohn, M. D., Hendrix, N., Penly Hall, G., &Lizotte, A. J. (Eds.). (2019). *Handbook on Crime and Deviance*.Handbooks of Sociology and Social Research.

Chang, J. (2008). An analysis of advance fee fraud on the internet. *Journal of Financial Crime* 15(1): 71–81

Cherry, K. (2020). Introduction to research methods: theory and hypothesis. Retrieved from https://www.library.sacredheart.edu

Chris Ngige, (2019). "Nigeria's unemployment rate hits 33.5 percent by 2020 – Minister | Premium Times Nigeria," May-2019. [Online], Available:https://www.premiumtimesng.com/news/top-news/328137-nigerias-unemployment-rate-hits-33-5-per-cent-by-2020-minister.html.[Accessed: 29-Jul-2020].

Clarke, R., &Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to do about It. New York: Harper Collins Publishers.

Cross, C.; Smith, R. G. & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends & issues in crime and criminal justice* no. 474. https://aic.gov.au/publications/tandi/tandi474

Doring N. M. (2009). 'The Internet's impact on sexuality: A critical review of 15 years of research'. Computers in Human Behavior. Vol. 25, Issue 5, pp.1089-1101.

Eze-Micheal, C. (2021). Causes and Effects of Cybercrime in Nigeria: An Examination of Socio-Economic, Legal, and Technological Factors. *Journal of Cybersecurity and Mobility*, 10(4), 479-508. https://doi:10.13052/jcsm2245-1439.1049

Ewepu G, (2016) Nigeria loses N127bn annually to cyber-crime — NSA available at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

Folashade B. O. &Abimbola K. A, (2015) 'Nature, Causes, and Consequences of Fraud Among Nigerian Youths and its Effect on Nigeria's Global Image. *International Journal of Intellectual Discourse* (IJID), Volume 3(2):409-421.

Furnell, S. (2020) "Technology Use, Abuse, and Public Perceptions of Cybercrime," in the Palgrave Handbook of International Cybercrime and Cyberdeviance, Springer International Publishing, pp. 45–66.

Ilievski, A. (2016). An Explanation Of The Cybercrime Victimisation: Self-Control And Lifestyle/Routine Activity Theory. *Innovative Issues and Approaches in Social Sciences*, Vol. 9, No. 1, pp.30-47.

Juan, H., Andrea, T., Pep, V., & Alberto, U., (2022) Smartphone Addiction, Social Support, and Cybercrime Victimization: *A Discrete Survival and Growth Mixture Model*. Psychosocial Intervention 31(1) 59-66.

Kamruzzaman, M., Islam, M. A., Islam, M.S., Hossain, M. S. & Hakim, M.A. (2016).Plight of Youth Perception on Cyber Crime in *South Asia American Journal of Information Science and Computer Engineering*. Vol. 2, No. 4, pp. 22-28.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries.*Social Science Computer Review*, 30(4), 470 – 486.

Kortjan, N., &Solms, R.V. (2014).A conceptual framework for cyber-security awareness and education in Nigeria. SACJ, 52, 29-41

Kranenbarg, M. W., Holt, T. J. & van Gelder J.L. (2019).Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap, Deviant Behavior,40:1, 40-55.

Lawanson J. &Afolabi M. B. (2020). Chasing the Nigerian Dream: The Proliferation of Cyber

Longe, O. B., &Chiemeke, S. C. (2008). Cybercrime and Criminality in Nigeria – What Roles are Internet Access Points Playing? European Journal of Social Sciences, 6(4), 132-139.

Lusthans, J. (2013). How organized is organized cybercrime? Global Crime, 14(1), 52-60.

Marshall, C &Rossman, G. (2014).*Designing qualitative research*: 6th edition.Sage publications.

Meško, G. (2018). On Some Aspects of Cybercrime and Cyber Victimization.*European Journal of Crime, Criminal Law and Criminal Justice*, 26(3), 189–199.

McQuade, S.C. (2006). *Understanding and Managing Cybercrime*. New York: Allyn and Bacon.

Moore, R. (2014). *Cybercrime: Investigating High-Technology Computer Crime*. Anderson.

Muktar, B. (2018) *Investigating Cybercriminals in Nigeria: A Comparative Study*. Salford Business School College of Business and Law University of Salford, UK

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5,773–793

N. Gershenfeld, R. Krikorian, & D. Cohen, (2004). "The Internet of things", Scientific America, vol. 291, no. 4, pp. 76-81,

Odumesi J. O., (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria, *International Journal of Sociology and Anthropology* 2014Vol. 6(3), pp. 116-125.

Ojedokun, U. A., &Eraye M. C. (2012). Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. *International Journal of Cyber Criminology*, 6(2), 1001–1013.

Otabor, J.O & Kinsley, O. (2016). Statistical approach to the link between internal service quality and employee satisfaction: a case study. *American journal of applied mathematics and statistics*. 4(6):178-184

Philip, N. N., Emmanuel, U. M., Igbo, &Uzoma, O. O. (2013). Cyber Crime Victimization among Internet active Nigerians: An Analysis of Socio-Demographic Correlates. *International Journal of Criminal Justice Sciences* Volume 8 Issue 2.

Rusch, J. J. (1999). The social engineering of internet fraud. In: Internet Society Annual Conference, http://www. isoc. org/

Shabnam, N., Faruk, M. O. &Kamruzzaman, M. (2016).Underlying Causes of Cyber-Criminality and Victimization: *An Empirical Study on Students. Social Sciences*. Vol. 5, No. 1, pp. 1-6.

Singh, P. A. (2014). Cyber Crime: Challenges and its classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), (*3) 119-121.

Singh, M.S (2016). Methodology series. Retrieved from https://www.pubmed.ncbi.nlm.nihgov

Song, H., Lynch, M.J. & Cochran, J.K. (2015).A Macro-Social Exploratory Analysis of the Rate of Interstate Cyber-Victimization. *American Journal of Criminal Justice*.1-20.

Suleiman, Ishaq, &Rabiu, B.I (2017), "The Nigerian Cybercrime (Prohibition,

Prevention, Etc.) Act 2015" in P.N. Ndubueze (Ed.). *Cyber Criminology & Technology Assisted Crime Control: A Reader. Zaria*: Ahmadu Bello University Press.

Umaru, I. (2020). The Impact of Cybercrime on the Nigerian Economy and Banking Undergraduates in Nigeria. *International Journal of Cyber Criminology* 5, 860-875

UNODC (2013).Comprehensive Study on Cybercrime. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/C

Voice of Nigeria (VON) (2023). Cybercrime: Gombe Governor urges collaborative effort security agencies to reduce cybercrime. www.von.org.ng

Williams, M. L. (2016). Individual and Environmental Influences on Online Criminal Engagement: An Examination of Routine Activity and Social Learning Theories. *Deviant Behavior,* 37(7), 730-747.