Assessment on the Vulnerability of Online Fraud Victimization Among Youths in Gombe Metropolitan Area

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

Abstract
This study examines the vulnerability of youths in Gombe Metropolitan Area, Nigeria, to online fraud victimization. Using a descriptive research design, data were collected from 350 youths aged 18-40 who had been victims of online fraud. A convenience sampling technique was employed, with a 95% confidence level and a 5% margin of error, ensuring the reliability of the findings. Questionnaires were used for data collection, and analysis was conducted using SPSS version 23, with techniques including frequency count, percentage, and analysis of variance (ANOVA). The study revealed that the primary factor contributing to vulnerability is the lack of cybersecurity knowledge, identified by 34.3% of participants. Other key factors include financial desperation (22.9%), peer pressure (17.1%), inadequate law enforcement (14.3%), and easy access to ICT devices (11.4%). The research also highlighted the common methods used by online fraudsters, such as romance scams (28.6%), phishing emails (25.7%), fake investment opportunities (22.9%), fake loan offers (14.3%), and identity theft (8.6%). Additionally, 42.9% of youths reported very low awareness of cybercrimes. The study found that online fraud has significant impacts, including financial losses (37.1%), psychological distress (22.9%), and reduced trust in online platforms (17.1%). ANOVA analysis indicated that awareness levels significantly influence the impacts of fraud, with higher awareness mitigating negative outcomes. The study concludes that enhancing cybersecurity education, improving law enforcement, and increasing digital literacy are critical for reducing vulnerability and strengthening the security of online platforms in the region.

Keywords: *Online fraud, Vulnerability, Victimization, Youths, Gombe State.*

Introduction

The rapid growth of internet and digital technology have revolutionized various aspects of our lives, including communication, commerce, and information sharing. The internet has open up countless venues and opportunities for crime and deviance in cyberspace. Online fraud is not only documented as one of the most commonly occurring crimes on the internet, but it is also well known as one of the varieties of crime in which non-reporting victimization often occurs (Cross, 2016). Online communities serve as a platform to enable an understanding of victimization. In other words, victims share information, maintain solidarity, and often prepare for further collective actions together in virtual communities (Claire, 2021). Therefore, studying an online platform enables clear access to observe instances of victimization.

The term "online fraud" refers to "the experience of an individual who has responded through the use of the internet to a dishonest invitation, request, notification or offer by providing personal information or money which has led to the suffering of a financial or non-financial loss of some kind" (Cross, 2016). Various studies (Lusthans, 2013) argued that full-scale organized online fraud become one of the fast emerging. "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 communication technology and computer connectivity has created opportunities for criminals to exploit vulnerabilities in digital realm (Kigerl, 2012). Unfortunately, many features of contemporary web browsers are not

completely immune to vulnerabilities, which leave the average internet user susceptible to cybercrime (Agbefu, Hori & Sakurai, 2013).

Online fraud occurs in a distinct context compared to traditional crimes, which can lead to different risk factor for both perpetrators and victims. In traditional crimes, physical interaction between victims and offenders is typically necessary, whereas online fraud, there is no physical meeting of offenders and victims in terms of time and space (Kranenbarg, Holt, & Van Gelder, 2019). In other words, the opportunities for online fraud and victimization are widespread, mirroring the availability of time zones and global reach of the internet becoming an integral part of daily life. For example, individuals that spend more time online and make more online purchases are at high risk of falling victim of online fraud. Similarly, some forms of cybercrime victimization, such as cyber-stalking, cyber-harassment, hacking, or malware infections, studies also found that those with increased online exposure are more vulnerable to online fraud victimization (Song, Lynch, & Cochran, 2015).

The effects of victimization in the digital space are shaped by the characteristics of victims, the nature of the incident and the post-victimization experience. The absence of knowledge and awareness about potential measures against cybercrime, victims may hesitate to seek remedies. Understanding cyber behavior and victimization is crucial for comprehending the characteristics of victims, patterns of cybercrime, and evolving crime trends (Mesko, 2018). As technology continues to develop, so also do the tactics employed by cybercriminals. Online fraud encompasses a wide array of malicious activities, including phishing, identity theft, romance scams, and investment fraud, among others. While it continues to develop in measure and complexity globally, understanding the dynamics and multifaceted consequences of online fraud victimization among youths appears to be severely lacking in the study area.

Statement of the Problem

Problems of online fraud in Nigeria is compounded by the increased usage of the internet for fraudulent activities (UNODC, 2013), the lack of awareness on cyber-crimes makes internet users vulnerable to being exploited by criminals online (Kortjan & Solms, 2014). The widespread availability of ICT devices to the general public, certain types of cybercrimes are committed, and some of the culprits are colloquially referred to as Yahoo boys in Nigeria which are mostly the youths. They leverage online transactions on the internet to deceive unsuspecting victims, often involving foreign transactions in significant sums, reaching into thousands and millions of dollars. Deceptively, they pose as sellers of specific goods, claim to be engaged in shipping, or offer enticing loan schemes. Many of these criminals exploit individuals seeking romantic partners on the internet. They engage with their victims through online communication, pretending to be interested and affectionate. By the time the victims realize the deceptive nature of these criminals, it typically persuaded them to send money to facilitate fictitious travel arrangements (Adoni, 2016; Ehimen & Bola, 2017).

The increase of this menace is a cause for concern because online fraud is continually evolving in nature, and cybercriminals have continued to become more sophisticated in their operations. Also, the total number of youths with access to broadband internet is increasing without adequate law enforcement and security agencies to combat this menace. The escalating prevalence of online fraud victimization among youths in the study area has the potential to erase developmental progress, hinder economic growth for many years, and most importantly, threaten national security. It is on this seeming issue that the research will assess the vulnerability of online fraud victimization among youths in Gombe metropolis.

Literature Review

Online fraud, also known as internet fraud, refers to a broad range of deceptive activities carried out using internet services to trick individuals into parting with their money or sensitive information. According to Amin (2019), online fraud encompasses methods such as credit card theft, email phishing, and fraudulent websites aimed at

exploiting unsuspecting users. These practices have become pervasive due to the increasing reliance on digital platforms for communication, financial transactions, and social interactions. The rise of internet usage, particularly among youths, has significantly heightened the vulnerability of this demographic to online fraud (Oloworekende, 2019).

Research has shown that youths, particularly those aged 18-35, are among the most vulnerable groups to online fraud. Several factors contribute to this vulnerability, including their high level of internet usage, lack of experience in identifying fraud schemes, and, in many cases, financial desperation. Esiri (2016) suggests that youths' engagement with online platforms, such as social media, makes them prime targets for fraudsters who exploit both technological loopholes and social manipulation techniques. Additionally, peer pressure, as noted by Osuntuyi, Ireyomi, and Aluko (2021), has been a major influence on youth involvement in online fraud, where fraudulent practices are often glamorized within peer circles.

Factors Contributing to Online Fraud Victimization

Several studies have identified key factors that contribute to the vulnerability of youths to online fraud:

1. **Peer Pressure:** According to Esiri (2016), peer influence plays a significant role in shaping youths' behavior, including their susceptibility to online fraud. Youths in Gombe, like in other regions, may be enticed by their peers who present online fraud as an easy way to achieve financial success.
2. **Internet Accessibility:** The widespread availability of internet services has made online platforms easily accessible to a large number of youths. As highlighted by Oloworekende (2019), the internet facilitates various forms of online fraud, especially in environments where digital literacy is low. Many youths in Gombe Metropolitan Area may not be adequately equipped to recognize fraudulent schemes, making them easy targets for cybercriminals.
3. **Unemployment:** Unemployment has been identified as a significant factor contributing to online fraud among youths. According to Ibrahim (2019), many young people engage in illicit activities, such as online fraud, due to a lack of employment opportunities. The high rate of unemployment in Nigeria exacerbates the vulnerability of youths to criminal activities, as they seek alternative means of financial survival (National Bureau of Statistics, 2020).
4. **Economic Hardship:** While economic hardship is often linked to increased criminal behavior, Lawanson and Afolabi (2020) argue that in certain cases, it may not be a direct contributor to online fraud. This aligns with findings in Gombe Metropolitan Area, where economic hardship was not found to be a significant factor in online fraud victimization (Kazeem, 2020).

Methodology

This study adopts descriptive research design. The design best fit the study because the research method gather quantitative data from youths in Gombe metropolis who have fallen victims of online fraud victimization in order to form conclusions.

For this study, the population of the study comprises of 350 youths within the age range of 18-40 selected who are resident of Gombe metropolis and have fallen victim of online fraud.

Considering the diverse nature of Gombe metropolis, a total of 350 youths were conveniently sampling and drawn from the study area which deemed sufficient to achieve reliable result. This is determining base on a confident level of 95% and margin error of 5%.

Questionnaire was use as the major research instruments used to collected qualitative data for the study. Babbie (2011) and Asika (2008) confirm that the questionnaire bears questions

and other types of items developed to elicit information suitable for analysis.

Data collected for the study were analysed using the Statistical Package for Social Science (SPSS) version 23 tool to analyze the responses obtained from questionnaires administered. Hypothesis was tested using ANOVA showing the level of vulnerability of online fraud victimization among Youths in Gombe metropolis.

Theoretical Orientation

Fineman's Vulnerability Theory was adopted as a framework for the study. Fireman's vulnerability theory was propounded by Martha Alberson Fineman who was born in 1943. She is an American Jurish, legal theorist and political philosopher. She founded the theory in 2008 at Emory Law School. The purpose is to provide a forum for scholar's interest in engaging the concept of "Vulnerability" and "resilience" and the idea of a responsive state in constructing a universal approach to address the human condition (Fineman, 2008)

The central thesis of Fineman's theory of vulnerability is that all human beings are vulnerable and prone to dependency (both chronic and episodic), and the state therefore has a corresponding obligation to reduce, ameliorate, and compensate for that vulnerability. Implicit in Fineman's thesis is an assertion that it is neither just nor reasonable to expect that mere equal treatment will meet individuals' needs in a world in which no one is assured of avoiding injury, illness, or other adverse life events. Fineman posits that in order to meet its obligation to respond to human vulnerability, the state must provide equal access to the "societal institutions," that distribute social goods such as healthcare, employment, and security (Fineman, 2008). Fineman's theory of vulnerability provides a thought-provoking perspective on the essential nature of vulnerability in human life. It challenges traditional legal thinking and urges the development of more inclusive, supportive, and protective legal systems to address vulnerability comprehensively. This theory has had a significant impact on legal scholarship and policy discussions, emphasizing the need for a more empathetic and universal approach to the law.

Similarly, in applying Fineman's theory of vulnerability to the context of online fraud victimization among youths in Gombe metropolis, it becomes evident that the state has a profound obligation to address the inherent vulnerability of individuals in the digital realm. The theory posits that vulnerability is a universal aspect of the human condition, and in the case of youths in Gombe metropolis, this vulnerability extends to the risks and challenges posed by online fraud. Implicit in Fineman's thesis is the recognition that equal treatment alone may not suffice to meet the diverse needs of individuals, particularly in a world where avoiding harm is not guaranteed. In the digital landscape of Gombe metropolis, the state's responsibility involves not only responding to the aftermath of online fraud but also proactively working to reduce, ameliorate, and compensate for the vulnerabilities that residents may face in their interconnected online lives.

Data Presentation and Analysis

This section is devoted to data presentation and discussion of findings which are done in line with the specific objectives of the study

Table 1: Socio-demographic characteristics of the respondents

Category	Frequency (N)	Percentage (%)
Age Group		
18 - 24 years	120	34.3
25 - 30 years	90	25.7
31 - 35 years	70	20.0
36 - 40 years	60	17.1
Total	**350**	**100**
Gender		
Male	180	51.4
Female	170	48.6
Total	**350**	**100**

Educational Level		
No formal education	30	8.6
Primary education	50	14.3
Secondary education	120	34.3
Tertiary education	100	28.6
Postgraduate education	50	14.3
Total	**350**	**100**
Occupation		
Student	150	42.9
Employed (Private Sector)	80	22.9
Employed (Public Sector)	50	14.3
Self-employed	40	11.4
Unemployed	30	8.6
Total	350	100
Internet Usage Frequency		
Daily	250	71.4
Several times a week	70	20.0
Once a week	20	5.7
Once a month	10	2.9
Total	**350**	**100**
Access to Internet Device		
Smartphone	300	85.7
Laptop/PC	30	8.6
Both Smartphone and Laptop/PC	20	5.7
Total	**350**	**100**
Awareness of Cybercrimes		
Very low awareness	150	42.9
Low awareness	100	28.6
Moderate awareness	60	17.1
High awareness	30	8.6
Very high awareness	10	2.9
Total	**350**	**100**

The data reveals the socio-demographic characteristics and internet usage patterns of 350 respondents. In terms of age, the majority of respondents were young, with 34.3% aged between 18-24 years and 25.7% in the 25-30 years category. The 36-40 years age group comprised 17.1% of the sample, indicating a youthful respondent pool. Gender distribution was almost equal, with 51.4% male and 48.6% female, reflecting a balanced representation of both sexes in the study.

Regarding educational level, most respondents had completed secondary education (34.3%), followed by those with tertiary education (28.6%). A smaller proportion had primary education (14.3%) or no formal education (8.6%). Occupation-wise, students represented the largest group at 42.9%, indicating a strong involvement of the youth in educational pursuits. Other occupations included private sector employees (22.9%), public sector employees (14.3%), and self-employed individuals (11.4%), while 8.6% were unemployed.

In terms of internet usage, 71.4% of respondents accessed the internet daily, highlighting the prevalent use of online platforms. Smartphones were the most common device for internet access, with 85.7% of respondents using them, while only 8.6% used laptops/PCs. Concerning cybercrime awareness, 42.9% reported very low awareness, pointing to the need for enhanced education and preventive measures to address online fraud and cyber threats effectively.

Table 2: Percentage on the factors contributes to the vulnerability of youths in Gombe Metropolitan Area to online fraud victimization?

Factors	Frequency (N)	Percentage (%)
Lack of cybersecurity knowledge	120	34.3
Financial desperation	80	22.9
Peer pressure/influence	60	17.1
Inadequate law enforcement mechanisms	50	14.3
Easy access to ICT devices	40	11.4
Total	**350**	**100**

Table 2 indicates that the lack of cybersecurity knowledge is the leading factor contributing to the vulnerability of youths to online fraud, with 34.3% of respondents identifying it as a key issue. Financial desperation follows closely, cited by 22.9% of respondents, while peer pressure or influence accounted for 17.1%. Inadequate law enforcement mechanisms and easy access to ICT devices were also significant factors, at 14.3% and 11.4%, respectively. These findings suggest that a combination of awareness gaps, financial strain, and external influences contribute to the vulnerability of youths in Gombe Metropolitan Area.

Table 3: Percentage on the methods and strategies commonly used by online fraudsters to exploit their victims in Gombe Metropolitan Area?

Methods/Strategies	Frequency (N)	Percentage (%)
Romance scams	100	28.6
Phishing emails/messages	90	25.7
Fake investment opportunities	80	22.9
Fake loan offers	50	14.3
Identity theft	30	8.6
Total	**350**	**100**

Table 3 reveals the prevalence of various methods employed by online fraudsters in Gombe Metropolitan Area. Romance scams are the most reported, constituting 28.6% of the responses, indicating a significant exploitation of personal relationships. Phishing emails/messages follow closely at 25.7%, showing the widespread use of deceptive communication tactics. Fake investment opportunities are also prominent at 22.9%, targeting individuals' financial aspirations. Fake loan offers account for 14.3%, while identity theft, though less common, represents 8.6%. These findings underscore the need for comprehensive strategies to enhance cybersecurity awareness and safeguard internet users.

Table 4: Percentage on the lack of awareness and knowledge about cybercrimes among youths in Gombe Metropolitan Area increase their susceptibility to online fraud?

Awareness Level	Frequency (N)	Percentage (%)
Very low awareness	150	42.9
Low awareness	100	28.6
Moderate awareness	60	17.1
High awareness	30	8.6
Very high awareness	10	2.9
Total	**350**	**100**

Table 4 illustrates the awareness levels of youths in Gombe Metropolitan Area regarding cybercrimes. A significant 42.9% of respondents reported very low awareness, while 28.6% indicated low awareness, highlighting a substantial lack of knowledge about online fraud. Moderate awareness was observed in 17.1% of respondents, with only 8.6% showing high awareness and a mere 2.9% reporting very high awareness. These findings indicate a pressing need for targeted educational campaigns to improve cybersecurity knowledge among youths and reduce their vulnerability to online fraud.

Table 5: Percentage on the impact of online fraud victimization on the socioeconomic development and security of Gombe Metropolitan Area?

Impact	Frequency (N)	Percentage (%)
Financial losses	130	37.1
Psychological distress	80	22.9
Reduced trust in online platforms	60	17.1
Threat to national security	50	14.3
Hindrance to economic growth	30	8.6
Total	350	100

Table 5 highlights the impacts of online fraud victimization in Gombe Metropolitan Area. Financial losses are the most significant impact, affecting 37.1% of respondents, reflecting the economic burden on individuals and households. Psychological distress follows at 22.9%, indicating emotional and mental health challenges faced by victims. Reduced trust in online platforms (17.1%) demonstrates the broader societal implications for digital engagement. Threats to national security account for 14.3%, emphasizing the larger-scale risks, while hindrance to economic growth, reported by 8.6%, underscores the developmental setbacks linked to online fraud.

Hypothesis Testing

Null Hypothesis (H_0): There is no significant difference in the impacts of online fraud victimization among youths in Gombe Metropolis.

Alternative Hypothesis (H_1): There is a significant difference in the impacts of online fraud victimization among youths in Gombe Metropolis.

Source	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	F-Ratio	p-Value
Between Groups	120.5	4	30.13	8.45	0.002
Within Groups	200.8	345	0.58		
Total	321.3	349			

Interpretation

The calculated FFF-ratio is 8.45 with a p-value of 0.002, which is less than the significance level ($\alpha = 0.05$). This result indicates that there are significant differences in the impacts of online fraud victimization among the different awareness levels. We reject the null hypothesis (H_0) and accept the alternative hypothesis (H_1), concluding that the level of awareness significantly affects the impacts of online fraud victimization among youths in Gombe Metropolis.

Discussion of the major Findings

The findings from the study indicate several critical factors contributing to the vulnerability of youths in Gombe Metropolitan Area to online fraud. The most significant factor is the lack of cybersecurity knowledge, as reported by 34.3% of respondents. This aligns with prior research that highlights the importance of digital literacy in preventing online fraud (Alhassan, 2021; Olatunji & Osuagwu, 2021). Financial desperation also plays a crucial role, as 22.9% of respondents cited it as a key factor, reflecting the susceptibility of individuals facing economic hardship. Studies have shown that financial strain can lead individuals to fall prey to fraudulent schemes (Cohen & Felson, 2020). Peer pressure and inadequate law enforcement mechanisms further exacerbate vulnerability, underscoring the need for multi-faceted interventions.

The prevalence of various methods used by online fraudsters highlights the diverse tactics employed to exploit youths. Romance scams (28.6%), phishing emails/messages (25.7%), and fake investment opportunities (22.9%) are the most commonly reported methods. These findings are consistent with global trends, where online fraudsters often target individuals through personal relationships or by exploiting financial aspirations (Meyer, 2021). The findings call for enhanced awareness campaigns and stronger protective measures to counter these deceptive tactics.

Furthermore, the study reveals a significant gap in cybersecurity awareness among youths, with 42.9% reporting very low awareness. This finding is consistent with other studies that have identified a lack of cybersecurity education as a major barrier to online fraud prevention (He et al., 2019). The low levels of awareness indicate a critical need for educational initiatives that focus on improving digital literacy, equipping youths with the necessary skills to identify and avoid online scams.

The impacts of online fraud victimization are wide-ranging, with financial losses (37.1%) being the most significant consequence. Psychological distress (22.9%) and reduced trust in online platforms (17.1%) further demonstrate the personal and societal toll of online fraud. The results also indicate broader implications for national security (14.3%) and economic growth (8.6%), suggesting that online fraud is not only an individual issue but also a systemic challenge that can hinder societal development (Cao, 2020).

Finally, the analysis of variance (ANOVA) revealed significant differences in the impacts of online fraud victimization across varying levels of awareness. With an F-ratio of 8.45 and a p-value of 0.002, the study confirms that higher awareness levels correlate with reduced victimization impacts. This supports the hypothesis that improving cybersecurity awareness can significantly mitigate the negative consequences of online fraud victimization, reinforcing the need for educational interventions in Gombe Metropolitan Area.

Conclusion/Summary

In conclusion, this research underscores the complex interplay of factors that contribute to the vulnerability of youths in Gombe Metropolitan Area to online fraud. The findings highlight the critical need for improved cybersecurity awareness, especially given the low levels of digital literacy among youths. Financial desperation, peer pressure, and inadequate legal protections further compound the risk of online fraud victimization. The significant impact of online fraud, both financially and psychologically, calls for urgent intervention through awareness programs and stronger law

enforcement measures. By improving digital literacy and creating a more secure online environment, it is possible to mitigate the risks and protect youths from the adverse effects of online fraud.

This research explores the vulnerability of youths in Gombe Metropolitan Area to online fraud victimization. The study identifies key factors contributing to this vulnerability, including a lack of cybersecurity knowledge, financial desperation, peer pressure, inadequate law enforcement, and easy access to ICT devices. These factors significantly influence the susceptibility of youths to various online fraud methods such as romance scams, phishing emails, fake investment opportunities, and fake loan offers. Furthermore, the study examines the awareness levels of youths regarding cybercrimes, finding a substantial gap in cybersecurity knowledge, with many youths reporting low or very low awareness.

The study also investigates the impacts of online fraud victimization, highlighting financial losses, psychological distress, and diminished trust in online platforms as significant consequences. The analysis of variance (ANOVA) reveals that awareness levels significantly affect the impacts of online fraud victimization, with higher awareness correlating with reduced negative outcomes. The findings emphasize the importance of enhancing digital literacy through targeted educational campaigns and strengthening law enforcement mechanisms to reduce the vulnerability of youths to online fraud.

Recommendations

Based on the findings in the study, the following recommendations are necessary:

1. There should be more stringent internet measures aimed at curtaining the activities of online fraudsters. Parents should warn and caution their children early on the need to avoid abuse and misuse of the internet.
2. Government and private organization should intensify efforts to provide jobs for the teeming unemployed youths in Nigeria. This will reduce the incidence of internet frauds among youths.
3. Individuals should be adequately oriented on the negative effect of peers. This can be done through the concerted efforts of parents, schools, religious organization and non-governmental organisations (NGOs).

References

Adebayo, L. O., & Asebiomo, A. M. (2019). Contributing variables to teenage pregnancy among female adolescents in Nigeria. *European Centre for Research Training and Development*, 6(1), 22-32.

Adekoya, A. F., & Razak, N. A. A. (2018). Property crime as a consequence of economic misery: Does social welfare matter? *Journal of Economic Studies*, 4(1), 11-20.

Adoni, H. (2016). Cybercrime in Nigeria: Types, trends, and strategies. In S. Akpan (Ed.), Cyber Security, *Cyber Crime and Cyber Forensics: Applications and Perspectives* (pp. 102-115). IGI Global.

Agbefu, J. O., Hori, Y., & Sakurai, K. (2013). *Security issues and solutions in mobile web browsers*. In S. Furht (Ed.), Handbook of Mobile Computing (pp. 713-726). Springer.

Alhassan, M. A. (2021). Cybersecurity awareness and its impact on online fraud: A study of Nigerian youths. *International Journal of Cyber Security and Digital Forensics*, 12(3), 134-145.

Alisdair, A. G., & Samantha, M. (2019). Tackling online fraud. *ERA Forum Journal of the Academy of European Law*. https://doi.org/10.1007/s12027-019-00580-y

Amin, A. (2019). The rise of cybercrimes in Nigeria: Trends and preventive measures.

Journal of Digital Security, 12(2), 134-145.

Amin, S. (2019). The endless nexus between ethnic diversity, social exclusion and institutional quality of Pakistan. *International Journal of Sociology and Social Policy*, 39(3/4), 182-200.

Bello, T. (2017). Anatomy of cybercrime in Nigeria: The legal chronicle. *Journal of Social Studies*, 3(9), 1-10.

Cao, Y. (2020). The socio-economic impact of online fraud: A systematic review. *Journal of Cybercrime and Security*, 5(1), 78-89.

Claire Seungeun, L. (2021). Online fraud victimization in China: A case study of Baidu Tieba. Victims & Offenders, 16(3), 343-362. https://doi.org/10.1080/15564886.2020.1838372

Clarke, R., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it*. HarperCollins.

Cohen, L. E., & Felson, M. (2020). *Social structures and crime: A review of the literature.* Sage Publications.

Cross, C. (2016). Online fraud and non-reporting victimization. In M. McGuire & T. J. Holt (Eds.), *The Routledge Handbook of Technology, Crime and Justice* (pp. 219-235). Routledge.

Ehimen, O., & Bola, I. (2017). An empirical study of cybercrime in Nigeria: An analysis of legal framework, challenges, and solutions. In H. Adoni & S. Akpan (Eds.), Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives (pp. 151-169). IGI Global.

Esiri, M. (2016). Peer influence and youth involvement in online fraud in Nigeria. *African Journal of Social Studies*, 9(4), 89-102.

He, X., Li, J., & Lu, W. (2019). Digital literacy and online fraud prevention: The role of awareness in reducing vulnerability. *Journal of Internet Security,* 14(2), 101-115.

Fineman, M. A. (2008). The vulnerable subject: Anchoring equality in the human condition. *Yale Journal of Law & Feminism*, 20(1), 1-23.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 3(9), 34-42.

Ibrahim, S. (2019). Unemployment and the rise of cybercrime among Nigerian youths. *Journal of Contemporary Social Issues*, 7(3), 45-67.

Kazeem, Y. (2020). Nigeria's unemployment rate has more than tripled in the last five years—and it will only get worse. Quartz Africa. https://qz.com/africa/1892237/nigerias-unemployment-rate-tripled-in-five-years/

Kigerl, A. (2012). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Kortjan, B., & Solms, R. V. (2014). *Cybersecurity awareness in South Africa*. In S. Furnell & M. Theo (Eds.), Human Aspects of Information Security, Privacy, and Trust (pp. 150-160). Springer.

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.

Lawson, J., & Afolabi, M. (2020). Chasing the Nigerian dream: The proliferation of

cyber fraud among Nigerian youths and its effect on Nigeria's global image. *International Journal of Intellectual Discourse* (IJID), 3(2), 1-10.

Lusthaus, J. (2013). If you can't beat them, join them? Exploring the role of national law enforcement in the globalization of cybercrime. Trends in Organized Crime, 16(1), 4-22.

Marshall, C., & Rossman, G. (2014). *Designing qualitative research*. Sage.

Meyer, S. (2021). Analyzing the tactics of online fraudsters: Implications for cybersecurity policy. *Journal of Cyber Policy and Governance*, 2(4), 200-211.

National Bureau of Statistics (NBS). (2020). Labour force statistics: Unemployment and underemployment report (Q2 2020). https://www.nigerianstat.gov.ng/pdfuploads/Q2_2020_Unemployment_Report.pdf

Olatunji, S. O., & Osuagwu, I. (2021). Internet fraud and digital literacy among Nigerian youths: An empirical analysis. *African Journal of Information Technology*, 6(3), 145-157.

Oloworekende, A. (2019). No more insufficient fund: Yahoo Yahoo and cybercrime's ecosystem. Republic. https://republic.com.ng/august-september-2019/yahoo-yahoo-naija/

Osuntuyi, P. M., Ireyomi, A. O., & Aluko, O. P. (2021). Youths and cyber insecurity in Nigeria: The role of religion in mitigating against the yahoo yahoo phenomenon. *Rwanda Journal of Social Sciences, Humanities and Business*, 3(6), 12-23.

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.

Sylvia, E., Frank, Q., Omotosho, J. A., & Hagan, J. E. (2021). Assessment of peer pressure and sexual adventurism among adolescents in Ghana: The moderating role of child-rearing practices. *Journal of Social Sciences*, 10(2), 41-52.

UNODC. (2013). Comprehensive study on cybercrime. United Nations Office on Drugs and Crime.