



Research article

UDC 34:004:343.9:004.8

EDN: <https://elibrary.ru/jvglrh>

DOI: <https://doi.org/10.21202/jdtl.2024.44>

Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization

Aminu Muhammad Auwal

University of Jos, Jos, Nigeria

Suleman Lazarus 

London School of Economics and Political Science, London, United Kingdom

University of Surrey, Guildford, United Kingdom

University of Portsmouth, Portsmouth, United Kingdom

Keywords

cybercrime victim,
cybercrime,
cybercriminology,
cyber-espionage,
digital criminology,
digital technologies,
legal policy,
online fraud,
victimization,
victimology

Abstract

Objective: to identify the main issues of victimization as a result of cybercrime growth in the world in general and in Nigerian society in particular from the standpoint of sociological approaches, using a Tripartite Cybercrime Framework (TCF), which comprises geopolitical, psychosocial and socio-economic categories of cybercrime.

Methods: the methodology is based on the sociological research method. The data collection included the distribution of a questionnaire among 896 participants from the academic environment, including students and university staff, and the analysis of the responses. The presented data were analyzed using descriptive statistics, with special attention to the issues of gender inequality, socio-economic factors, the impact of educational level on vulnerability to online fraud and victimization as a result of cybercrime through the prism of the ideal victim concept and the socio-economic gap between North and South.

Results: the article presents an analysis of the Tripartite Cybercrime Framework. The survey showed that 65.20% of the participants had been victims of cybercrime. There were more men among the victims (64.69%). The authors found patterns in the distribution of cybercrimes. All cybercrimes against the respondent were socio-economic ones, which underlines the

 Corresponding author

© Auwal A. M., & Lazarus S., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

high frequency of cybercrime and the relevance of countering it in Nigerian society. Special attention was paid to the issues of gender inequality, socio-economic factors, and the impact of education on vulnerability to cybercrime. The article considers from the viewpoint of the ideal victim concept. The study results provide an idea of the prevalence and distribution of specific types of cybercrime in the socio-economic category among the studied population.

Scientific novelty: For the first time, the study uses the Tripartite Cybercrime Framework (TCF) to study victimization as a result of cybercrime in Nigerian society. The research novelty is also due to the fact that the conceptual foundations of countering cybercrime that have developed in the global North are not fully applicable in Nigeria.

Practical significance: the results obtained demonstrate the need to apply carefully calibrated gender-based, inclusive and contextual approaches to the development of a national legal policy to combat cybercrime. The results can be used to justify the law-making decisions which are being developed in the field of preventing and countering manifestations of cybercrime, as well as to form the basis for legal measures to protect cybercrime victims.

For citation

Auwal, A. M., & Lazarus, S. (2024). Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization. *Journal of Digital Technologies and Law*, 2(4), 915–942. <https://doi.org/10.21202/jdtl.2024.44>

Content

Introduction

1. Literature Review

1.1. Cybercrime and Cyber Criminology

1.2. Tripartite Cybercrime Framework (TCF)

1.2.1. Geopolitical Cybercrime

1.2.2. Psychosocial Cybercrime

1.2.3. Socioeconomic Cybercrime

1.3. Complexities and Challenges of Cybercrime in Nigeria

1.4. The Rise of Economic Cybercrime in Nigeria

1.5. Victims-Oriented Studies

1.6. Cybercriminals in a Nigerian society (Yahoo Boys)

1.7. Convergence and Divergence in Prior Research

1.8. Novelty of Current Work

2. Methods and materials
 - 2.1. Data Analysis
 3. Results
 - 3.1. Gender Dimension
 - 3.2. Educational Level
 - 3.3. Confirmed Negative Experience of Cybercrime
 - 3.4. Type of Cybercrime
 - 3.5. Reported Incidents
 - 3.6. Stolen Money Reversed/Suitable Action Taken
 4. Discussion
 - 4.1. Gender Dimension of Online Fraud Victimization
 - 4.2. The centrality of Socioeconomic Dynamics of Cybercrime
 - 4.3. Educational Attainment and Online Fraud Victimations
 - 4.4. Cybercrime Victimization, Ideal Victims, and the North-South Divide
- Conclusion
- References

Introduction

While cybercrime is a global issue, spatial characteristics influence local human behavior and can be revealed or hidden by spatial elements (Hall & Yarwood, 2024; Lazarus & Button, 2022). This article aims to shed light on the reported cybercrime experiences and provide empirical evidence through quantitative analysis. Cybercrime has emerged as a significant societal concern in Nigeria, and its prevalence has increased in recent years (Ibrahim, 2016a; Idem & Olarinde, 2023). Many scholars have examined victims of cybercrime in various contexts, such as Australia (Cross, 2020; Drew & Webster, 2024), China (Wang, 2023), Portugal (Murça et al., 2024), the United Kingdom (Lazarus et al., 2022b) and Russia (Timofeyev & Dremova, 2022). Only a few studies have investigated the victims of cybercrime in Nigeria. Unlike in many nations, especially such as Australia (Cross, 2020; Drew & Websters, 2024; Meikle & Cross, 2024) and the United Kingdom (Button et al., 2014, 2015; 2021), victims of cybercrime in Nigeria are under-researched.

For instance, Aborisade et al. (2024) conducted a study through interpretative phenomenological analysis and one-on-one semi-structured video interviews; ten victims of Nigerian romance fraudsters from six different nations were examined. In addition, Tade and Adeniyi (2017) examined data generated through in-depth interviews with ATM fraud victims, revealing that victims suffered post-fraud trauma and often relied on friends, parents, and relatives to cope with the aftermath. However, none of these studies utilized quantitative methods to explore respondents' demographic

characteristics and experiences of cybercrime. This study aims to address this gap by investigating the demographic characteristics and experiences of respondents regarding cybercrime. Specifically, it sought to examine the prevalence, characteristics, and reporting dynamics of cybercrime experiences among respondents. To achieve this, the study aims to contribute to the under-researched topic of cybercrime victimization in Nigerian society using data collected via a distributed survey.

1. Literature Review

1.1. Cybercrime and Cyber Criminology

The idea that the division between the physical and digital worlds hinders the understanding of offline social cues, which also affect the digital realm, has been explored by various scholars (Jaishankar, 2007; Ibrahim, 2016a; Powell et al., 2018). While researchers have emphasized the connection between offline and online life, they have used different terms to convey this concept. For instance, McGerty (2000) stated that «nobody lives only in cyberspace,» Jaishankar (2007, 2011, 2018) introduced the concept of «cyber criminology,» while Powell et al. (2018) rebranded it «digital criminology». These variations in terminology reflect the contestation of ownership within scholarly discourse on this topic.

The concept of «cybercrime» encompasses unlawful activities conducted via the Internet and Information Communication Technology (ICT), including «cyber-dependent» and «cyber-enabled crimes» (Button et al., 2023; Ibrahim, 2016a; Hall & Yarwood, 2024; Musotto & Wall, 2022). While often used interchangeably to refer to all online unlawful activities, it is common for security agencies, researchers, and the media to group various digital offenses under «cybercrime,» ignoring their unique attributes (Lazarus, 2019). Cyber-dependent offenses occur even without digital technology or networks, while cyber-enabled crimes are amplified by networks. We focus on cyber-enabled crimes. However, the conflation of «cyber-enabled crimes»¹ and «people-centric cybercrimes» (Gordon & Ford, 2006) makes it difficult to differentiate financially motivated crimes like «online fraud» from psychologically motivated ones like «revenge pornography» (Ibrahim, 2016a; Lazarus, 2019). We now utilize Nigerian-oriented frameworks and perspectives on cybercrime, particularly Ibrahim (2016a), to contribute to ongoing discussions on online fraud victimization, addressing the oversight of Nigerian scholars' insights, as Cross (2018a) pointed out.

¹ McGuire, M., & Dowling, S. (2013, October). Cybercrime: a review of the evidence: Research Report 75. <https://clck.ru/3F25c7>

1.2. Tripartite Cybercrime Framework (TCF)

Empirical literature (De Kimpe et al., 2020; Lazarus et al., 2022b) has utilized the Tripartite Cybercrime Framework (TCF) to distinguish between cybercrimes driven by psychology (psychosocial cybercrime), economics (socioeconomic category), and geopolitics, as illustrated in Fig. 1, derived from Ibrahim's (2016a) original formulation. Ibrahim (2016a) specifically clarifies that while cybercrimes in a Nigerian context are primarily financially driven, not all cyber-enabled crimes, such as revenge pornography, possess this attribute. Drawing from these classifications, we highlight the unique characteristics of cybercrimes in Nigeria as a subset of offenses. Cybercrime is indeed a global crime. However, it also exhibits spatial characteristics, influencing human behavior in specific regions and manifesting in spatial elements that may be concealed or revealed (Hall & Yawood, 2024; Lazarus & Button, 2022).

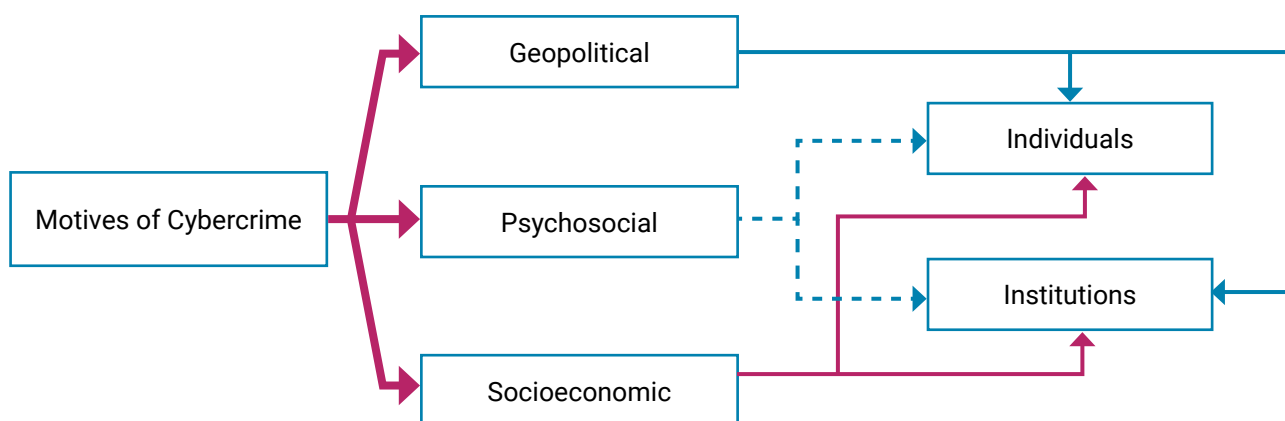


Figure 1. Tripartite Cybercrime Framework (TCF)

1.2.1. Geopolitical Cybercrime

Geopolitical cybercrime involves cybercrimes driven by political motives, often involving state actors, non-state activists, or their representatives (Ibrahim, 2016a; Lazarus, 2019). These activities may include cyber espionage or attacks on critical infrastructure. However, cybercrime originating from Nigeria rarely falls into this category, unlike other nations such as the United States and China (Ibrahim, 2016a). For instance, state-sponsored hacking groups may target foreign government agencies to gather intelligence for political advantages in diplomatic negotiations or military strategies (Akoto, 2021; Makridis et al., 2024). The primary motivation for geopolitical cybercrime is political, aligned with the geopolitical category of TCF (Ibrahim, 2016a).

1.2.2. Psychosocial Cybercrime

Psychosocial cybercrime involves digital offences primarily driven by psychological motivations, intending to cause distress, anguish, or harm to individuals (Ibrahim, 2016a; Lazarus, 2019). Monetary gain is not the primary objective in such cases. Examples include cyberstalking, cyberbullying, and online abuse, targeting victims on social media platforms to harm them psychologically and undermine their credibility. Perpetrators derive satisfaction from causing distress, emphasizing the psychosocial nature of these crimes (Ibrahim, 2016a; Lazarus, 2019). While revenge pornography offenders often blame and humiliate victims, this is not the primary motive for fraud, which is money.

1.2.3. Socioeconomic Cybercrime

Socioeconomic cybercrime involves the pursuit of financial gains through deceptive practices facilitated by computers or internet technologies. This encompasses illegal activities such as online fraud, romance scams, copyright theft, and illegal downloads of digital content (Ibrahim, 2016a). Nigeria is particularly vulnerable to practices within this category, which include prevalence, impersonation, manipulation, counterfeiting, forgery, and fraudulent misrepresentation. Notable examples include online romances (Drew & Webster, 2024; Lazarus et al., 2023) and pig butchering fraud (Wang, 2023; Whittaker et al., 2024). These fraudulent schemes are primarily motivated by financial gain.

However, the geopolitical, psychosocial, and socioeconomic categories are not rigidly defined, and instances of overlap can occur. For example, hacktivists may release stolen personal information to convey political messages, which has psychological and geopolitical implications. Nonetheless, the TCF serves as a useful tool for categorizing the distinct characteristics of various cybercrimes in Nigeria and beyond. Nigeria lacks substantial documentation of other types of cyber offences, such as cyber espionage, cyberstalking, and revenge porn, which are more prevalent in countries such as Belgium, Canada and the United Kingdom (Ibrahim, 2016a). Therefore, the conceptual framework of the cybercrime framework in the Global North may not fully apply in Nigeria, representing Africa south of the Sahara (Ibrahim, 2016a). The complexities of cybercrime in Nigeria are worth noting.

1.3. Complexities and Challenges of Cybercrime in Nigeria

Recent conference papers shed light on various aspects of cybercrime prosecution, regulation, and its impact on Nigeria. Idem et al. (2023a) identified key challenges hindering cybercriminal prosecution in Nigeria, including the lack of robust legislation,

ineffective law enforcement, slow legal processes, and limited forensic analysis capabilities. Building on this, Idem et al. (2023b) emphasize the urgent need for reform within cybercrime regulatory agencies to protect Nigeria from its status as one of the top three countries with the highest growth of cybercrime. Similarly, Idem (2023) suggests that Nigeria's Cybercrimes Law has played a significant role in regulating and deterring various forms of cybercrime, safeguarding online businesses, and promoting internet enterprises. These three related studies collectively spotlight the multifaceted challenges posed by cybercrime in Nigeria and emphasize the importance of legislative, regulatory, and socioeconomic interventions to address them.

Furthermore, while Ojolo and Adewumi (2020) and Lazarus et al. (2023) illuminate the normalization of cybercrime within Nigerian society, highlighting factors such as economic instability, corruption, and peer influence as significant drivers of its prevalence, Lazarus et al. (2022a) draws parallels between internet scammers (Yahoo Boys) and Nigerian corrupt politicians ("Yahoo Men"). Similarly, Olaiya, Lamidi, and Bello (2020), Monsurat (2020), and Adeduntan (2022) emphasize the influence of political corruption, peer pressure, economic hardship, and inadequate social support systems. Additionally, Ojolo and Singh (2023) and Aransiola and Asindemade (2011) uncovered the lucrative nature of this activity and the complicity of corrupt law enforcement officers and asserted that financial incentives intersect with institutional vulnerabilities to sustain illicit practices online. Collectively, the above studies suggest that cybercrime is a complex phenomenon rooted in socioeconomic disparities, institutional deficiencies, and cultural influences. Nonetheless, there is a clear pattern that incidents of cybercrime have risen in recent years.

1.4. The Rise of Economic Cybercrime in Nigeria

The Rise of Economic Cybercrime in Nigeria has become a concern for various stakeholders. Idem and Olarinde (2023) highlight the negative effects of cybercrime on youth development, the economy, and governance in Nigeria. They identify unemployment, poverty, corruption, and ineffective governance as primary drivers of youth involvement in cybercriminal activities and offer recommendations to combat these issues. According to the analysis of cybercrime and cybersecurity incident reports posted by the Economic and Financial Crimes Commission (EFCC) from 2019 to 2022, online fraud has been on a sharp rise². This is how this information is summarised to give the idea of cybercrime incidence in Nigeria, when the number of sentences dramatically increased in four years of observation.

² EFCC. (2022). <https://goo.su/TJjHS>

For example, between 2019 and 2022, the EFCC witnessed a substantial surge in reported cybercrime incidents. In 2019, 877 individuals reported cybercrime incidents, which escalated to 1890 incidents in 2020, representing a 115.5 % increase compared to the previous year. By 2021, reported incidents further rose to 2400, reflecting a staggering 173.7 % increase compared to the baseline of 2019. Projections for 2022 indicated a continued upward trend, with 2900 reported incidents comprising a substantial 230.7 % increase compared to the initial figures of 2019. These statistics highlight the exponential growth of online scams and underscore the exigency for scholarly inquiry into victimization patterns within the country. Our analysis reveals a marked surge in cybercrime activities, substantiated by the escalating number of convicted cybercrime incidents reported by the EFCC. These findings spotlight a significant uptick in cybercrime within Nigeria over the specified timeframe, emblematic of the activities of cybercriminal entities, predominantly recognized as Yahoo Boys (Aborisade, 2023; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012).

1.5. Victims-Oriented Studies

The actions of Yahoo Boys have global repercussions, prompting an increase in research focused on victims of online fraud. Many studies have been conducted on the topic of victimization, but most of them have focused on Western societies and Asian nations like China. A few studies have looked into African nations like Nigeria, but they are relatively uncommon. For instance, studies by Button et al. (2014), Meikle and Cross (2024), Drew and Websters (2024), Cross (2020), Cross (2018b), and Whitty (2019) primarily concentrate on victims from Western societies and Asian nations like China (Tao, 2022; Wang, 2023; Wang & Topalli, 2024), while only a few researchers such as Aborisade et al. (2024) have studied victimization in African nations like Nigeria. This imbalance could be stemming from the Western media's exclusive coverage of victims from Western countries, as well as priorities of research funding allocation. Such tendencies perpetuate and inadvertently marginalize victims from a Nigerian context. This study seeks to address this disparity by emphasizing that the detrimental impact of Yahoo Boys extends beyond local boundaries to the global arena. By shedding light on the experiences of victims in African nations like Nigeria, we aim to challenge the prevailing Western-centric narrative and highlight the universality of the issue. Through an inclusive approach, we endeavor to contribute to a deeper understanding of online fraud and its impact on victims worldwide.

1.6. Cybercriminals in a Nigerian society (Yahoo Boys)

Several qualitative investigations have investigated Nigerian cybercriminals both within Nigeria (Aransiola & Asindemade, 2011; Lazarus & Okolorie, 2019; Ogunleye et al., 2019; Ojedokun & Eraye, 2012) and outside Nigeria (Lazarus, 2024), thereby providing insights into the diverse facets of these offenders. The empirical literature cited above consistently

indicates that men (and boys) are the primary perpetrators of cybercrime. These individuals fundamentally coordinate socioeconomic digital crimes on the internet, as shown in Figure 1. In contrast to their male counterparts, according to testimonials, female undergraduates who commit online fraud mostly do so from subordinate positions to their male-dominated superior positions (Ogunleye et al., 2019). Although the research above findings specifically pertained to Nigerian society' emphasizing that males are the predominant perpetrators of these cybercriminal activities, only a limited number of studies, including Aborisade et al. (2024), have investigated the experiences of cybercrime victims in Nigeria.

1.7. Convergence and Divergence in Prior Research

In the Nigerian context, many research endeavors have produced convergent findings using a variety of data sources. These include interviews with frontline law enforcement officers (Lazarus & Okolorie, 2019), analysis of scam emails (Genc et al., 2021; Rich, 2018), examination of music lyrics (Adeduntan, 2022; Lazarus et al., 2023), interviews with Nigerian parents (Aborisade, 2023; Ibrahim, 2016b), interviews with online fraudsters (Aransiola & Asindemade, 2011; Lazarus, 2024; Ojedokun & Eraye, 2012; Ogunleye et al., 2019), exploration of tweets (Lazarus & Button, 2022), and consistency and concurrence among these studies substantially enhance the credibility of empirical research as a whole, thereby reaffirming the fundamental understanding about characteristics of online offenders and they category of cybercrimes they commit. Furthermore, studies not based on empirical evidence support the empirical literature (Idem et al., 2023a, 2023b). This verifies these attributes and brings together evidence from diverse research methodologies. Only a limited number of studies have been conducted on victims of cybercrime in Nigeria, notably Aborisade et al. (2024), Mba et al. (2017), and Tade and Adeniyi (2017).

1.8. Novelty of Current Work

This study is distinct from previous research in several respects. Although previous studies have investigated cybercrime victims in Nigeria (Aborisade et al., 2024; Mba et al., 2017; Tade & Adeniyi, 2017), no distributed questionnaires have been employed. Previous approaches, such as those by Aborisade et al. (2024) and Tade and Adeniyi (2017), relied on qualitative methods, whereas Mba et al. (2017) sourced data from a Nigerian forum hosted at www.topix.com, supplemented by Web engine searches to identify similar online and active scam posts. While empirical literature such as De Kimpe et al.'s (2020) study in Belgium has used the TCF as a reference point, none has ever examined cybercrime by explicitly considering the Tripartite Cybercrime Framework (TCF) excerpt for Lazarus et al. (2022b) study which merge the TCF and feminist epistemology of crime. While Lazarus et al. (2022b) explored perceptions of cybercrimes aligned with the TCF categories in the United Kingdom, our study aims to address this gap by examining cybercrime victimization in Nigeria through the lens of the TCF classifications. We will use «the Socioeconomic Theory of Nigerian Cybercriminals» proposed by Ibrahim (2016a) as a framework for our research.

2. Methods and materials

We employed a distributed survey approach to collect data from a diverse cohort of students, staff, and workers from various sectors. Our questionnaire explores Ibrahim's (2016a) framework, which categorizes cybercrime into socioeconomic, geopolitical, and psychosocial dimensions, to expose the nuances and particularities of cybercrime types in Nigeria. The survey targeted voluntary participants with diverse demographic backgrounds to contribute to the understanding of cybercrime experiences. While participants' responses were anonymized and kept confidential, ethical approval was obtained from one of the universities in Nigeria to ensure academic and research guidelines adherence. The survey was meticulously designed and distributed through established survey platforms to ensure its efficiency and broad reach. Participants provided informed consent before participation, and stringent measures were implemented to safeguard their anonymity and confidentiality throughout the data collection process.

2.1. Data Analysis

We conducted a nearest-neighbor analysis to identify the geographical clusters and sectors most affected by cybercrime. By employing a combination of simple statistical methods and advanced spatial statistics, data analysis yielded valuable insights into the prevalence and characteristics of cybercrime in the studied population. Moreover, statistical analysis was employed to discern trends and patterns in cybercrime occurrence rates over a specified period. Descriptive statistics such as means and medians were computed using Excel spreadsheets to facilitate the calculation of relevant counts and percentages. While this method has its limitations, however, we offer the following justifications for this approach:

1. Exploratory Analysis. Descriptive statistics serve as a valuable tool for conducting exploratory analysis, enabling researchers to gain an initial understanding of the data by summarizing key characteristics like central tendency and variability. Since this is a preliminary study, this approach allows for the identification of basic patterns in cybercrime experiences among participants without assuming underlying relationships, which may not be misleading, given the complex sociocultural fabric of Nigerian society.

2. Data Presentation. Descriptive statistics are crucial for presenting critical findings in a clear and concise manner, making them accessible to a broad audience, including undergraduate students from various disciplines. Given that the study focuses on cybercrime experiences among university students and workers in Nigeria, descriptive statistics provide a straightforward way to communicate important findings about the prevalence and characteristics of cybercrime in this population.

3. Simple Data Structures. The investigation tool used in the study has a relatively simple structure with few variables and straightforward relationships. As such, descriptive statistics are well-suited to address the research question and objectives

of this preliminary inquiry. More complex analytical techniques may not be necessary. They could introduce unnecessary complexity, making descriptive statistics an efficient way to analyze and summarize data, providing valuable insights into cybercrime victimization experiences among the study population.

3. Results

This section presents the findings from the quantitative analysis of 896 responses, delineating the frequencies and percentages associated with each category identified in the study as illustrated in Table 1. Almost all participants (99.78 %) provided informed consent, indicating a high level of willingness to participate in the study. Only a small fraction (0.76 %) chose not to provide consent, suggesting that most participants were willing to participate.

Table 1. Summary of Our Findings

Item	Type	Frequency	Percentage
Informed consent response	Yes	896	99.78
	No	7	0.76
Gender of the respondents	Male	584	64.69
	Female	312	34.52
Educational level	Masters' Students	522	57.80
	Doctoral Candidates	21	2.36
	Teachers and Admin Staff	12	1.35
Experience of cybercrime as victims	Yes	588	65.20
	No	301	33.40
Gender of cybercrime victims	Male Victims	303	51.53
	Female Victims	285	48.47
Type of Cybercrime	E-Banking/Payment-Card Fraud	554	61.45
	Identity Theft	67	7.43
	Others	295	32.68
Reported?	Yes	322	35.74
	No	577	63.94
Stolen Money reversed/Suitable Action Taken?	Yes	54	5.99
	No	835	92.61

3.1. Gender Dimension

The findings of this study shed light on the gender dynamics within cybercrime victimization, revealing a notable disparity in the experiences of men and women. Data analysis indicates that among individuals affected by cybercrime, 303 men (51.53 %) and 285 women (48.47 %) reported adverse outcomes. This disparity is further underscored by the overall distribution of cybercrime victims, with 64.69 % male and 34.52 % female. These figures suggest a gendered pattern in cybercrime

victimization, with a higher proportion of men experiencing negative consequences compared to women. The data also highlights the need for gender-sensitive approaches in addressing cybercrime and implementing interventions to mitigate its impact on both male and female victims. Additionally, the relatively balanced distribution between male and female victims underscores the importance of considering gender dynamics in understanding and responding to cybercrime phenomena.

3.2. Educational Level

The participants had a diverse range of educational backgrounds. 37.80 % were undergraduates, 57.80 % were master's students, 2.36 % were doctoral candidates, and 1.35 % were teachers and admin staff. This diversity in educational level enriches the sample's heterogeneity and makes the findings more generalizable.

3.3. Confirmed Negative Experience of Cybercrime

A significant proportion of participants (65.20 %) reported experiencing adverse incidents related to cybercrime, highlighting its pervasive impact on the study population. Conversely, 33.40 % indicated that they had not experienced any cybercrime incidents, revealing a subset of individuals unaffected by this type of crime.

3.4. Type of Cybercrime

The study found distinct prevalence patterns in cybercrime incidents. E-Banking/Payment-Card Fraud was the most common type, accounting for 61.45 % of reported incidents. Identity Theft accounted for 7.43 % of incidents, while other forms collectively constituted 32.68 % of cases, such as online job scams. These findings provide insights into the prevalence and distribution of specific cybercrime types among the study population: the socioeconomic types.

3.5. Reported Incidents

The study found that 35.74 % of participants reported cybercrime incidents to relevant authorities or entities, indicating a moderate engagement with reporting mechanisms. In contrast, the majority (63.94 %) did not report any incidents, suggesting potential underreporting and areas for improvement in reporting practices.

3.6. Stolen Money Reversed/Suitable Action Taken

Among participants who reported cybercrime incidents, only a minority (5.99 %) indicated that stolen funds were reversed or appropriate actions were taken in response. Conversely, the vast majority (92.61 %) reported no remedial actions, suggesting

challenges in achieving restitution or resolution following cybercrime victimization. While these findings provide valuable insights into cybercrime prevalence, characteristics, and reporting dynamics among participants, further exploration is warranted to compare with prior empirical literature and to discern implications for policy, practice, and future research endeavors.

4. Discussion

In the discussion section, we build upon insights garnered through a distributed survey approach to advance understanding cybercrime victimization across diverse demographic spectra. This section discusses four primary themes: (1) Disparities in Cybercrime Experiences based on gender; (2) the pivotal role of Socioeconomic pertaining to Cybercrime in Nigeria; (3) the correlation between Educational Attainment and vulnerability to online fraud; and (4) an exploration of Cybercrime Victimization through the lens of ideal victimization, juxtaposed with the North-South socioeconomic Divide.

4.1. Gender Dimension of Online Fraud Victimization

Our study's analysis of gender disparities in cybercrime victimization (Table 1, section 3.4 of the article) both aligns with and diverges from findings in prior research. For example, Lazarus et al. (2022b) assert that while women tend to perceive psychosocial cybercrimes, such as revenge pornography, as more severe than men, no discernible gender disparities exist in socio-economic cybercrimes like credit card online fraud. Notably, unlike the above authors, our study does not explicitly explore perceptions of cybercrime and shows a gender difference in socioeconomic cybercrime victimization, contributing to the discourse. Moreover, numerous studies have delved into the intricate dynamics of cybercrime victimization, shedding light on various influencing factors (Näsi et al., 2023). Kadoya et al. (2021) research in Japan identified gender and marital status as potential determinants of victimization, indicating that males and married individuals are more susceptible to fictitious billing fraud. Similarly, Whitty's (2019) study in the United Kingdom underscores gender variations in cybercrime, particularly evident in romance fraud, where women are disproportionately victimized. Although our study did not specifically inquire about marital status or romance scams, our findings resonate with those of Kadoya et al. (2021) and Whitty (2019), corroborating the significance of gender in cybercrime victimization.

The variability in gender disparities across different contexts is further illuminated by studies conducted in Finland (Näsi et al., 2023) and the Netherlands (Weijer et al., 2020). While Finnish research found no statistically significant gender differences, a Dutch study revealed that females were likelier to report traditional crimes to the police, while

males exhibited greater proactivity in reporting cybercrime incidents (Näsi et al., 2023; Weijer et al., 2020). Consequently, it is plausible to assert that the gender differences identified in our study may be attributed, in part, to disparities in crime reporting behavior. This underscores the multifaceted nature of cyber victimization reporting, often leading to cybercrimes being reported to organizations other than the police. Furthermore, gender differences significantly impact susceptibility to online fraud, with psychological traits such as risk-taking and low self-control further contributing to vulnerability (Norris et al., 2019). Although our study did not investigate psychological traits and their association with online fraud victimization, our findings agree that gender differences significantly influence susceptibility to online fraud. Despite these gender-related nuances, gender alone plays only a partial role in predicting cyber victimization, with other factors such as fraudster motivation and target vulnerability exerting considerable influence as well.

4.2. The centrality of Socioeconomic Dynamics of Cybercrime

Our research has identified clear prevalence trends in cybercrime incidents (Table 1), notably highlighting E-Banking/Payment-Card Fraud as the most dominant type, comprising 61.45 % of reported cases. Identity Theft comprised 7.43 % of incidents, while various other scams, including online job scams and phishing schemes, collectively accounted for 32.68 % of cases, all falling within the socioeconomic category of cybercrime (Table 1). It reinforces that cybercrime exhibits spatial characteristics as it traverses and manifests in various regions, exerting an impact on human conduct within particular localities while also being capable of being obscured or revealed by spatial elements (Hall & Yawood, 2024; Lazarus & Button, 2022). The Tripartite Cybercrime Framework (TCF) delineates cybercrimes into three principal motivational components – socioeconomic, psychological, and geopolitical – underscoring the distinction between socioeconomic and psychosocial cyber offenses (Ibrahim, 2016a; Lazarus, 2019; Lazarus et al., 2022b).

Unlike countries like Canada, Russia, China, and the United Kingdom, Nigeria lacks substantial documentation of other cybercrime categories, notably geopolitical, such as cyber espionage, and psychosocial, such as revenge pornography (Ibrahim, 2016a). The geopolitical and sociocultural contexts of different nations significantly shape their behavior in cyberspace. For instance, while revenge pornography is prevalent in Western nations like Portugal (Murça et al., 2024), the United Kingdom, Canada, etc. (Harper et al., 2023), it may not be as pronounced in Nigeria. Furthermore, unlike Nigeria, countries like the United States, Russia, China, and the United Kingdom confront significant challenges with nation-sponsored cyber espionage (Akoto, 2021, 2024; Markridis et al., 2024). These social and contextual nuances challenge the notion

of cyberspace and physical space as distinct entities with clear boundaries, as highlighted by Jaishankar (2007, 2011, 2018). As a result, the conceptual frameworks commonly utilized in “the Global North” may not entirely apply in Nigeria, representing Africa south of the Sahara (Ibrahim, 2016a). The complexities of cybercrime in Nigeria are notable. Although our survey data originated from a single institution, the findings offer insights into the prevalence and distribution of cybercrime types within the socioeconomic classification.

However, while Nigeria may lack substantial documentation of certain cybercrime categories, it does not necessarily mean that psychosocial cybercrimes, such as cyberstalking and cyberbullying, are non-existent or negligible. One possible explanation is that the sociocultural fabric of Nigerian society prioritizes socioeconomic cybercrime types, such as online scams. This emphasis is evident in the exclusive focus on financial crimes reported by the EFCC, the elite enforcement agency in Nigeria. Additionally, the lack of documentation could stem from other factors, such as limited resources or infrastructure for detecting and reporting such cybercrime types. Furthermore, while sociocultural and geopolitical contexts influence cyberspace behavior, it is essential to acknowledge that geopolitical cybercrime types often do not affect ordinary citizens like the students and teachers we studied in this research. As a result, our inquiry did not cover geopolitical entities, leading to potential oversight in our findings.

4.3. Educational Attainment and Online Fraud Victimization

One significant discovery from our research pertains to the educational backgrounds of the participants. While over 99 % of them possessed or were in the process of obtaining a university degree, the distribution across educational levels varied considerably. In particular, among the participants, 37.80 % were undergraduates, 57.80 % were master’s students, 2.36 % were pursuing doctoral degrees, and 1.35 % were educators and admin staff (Section 3.4 of the article). Despite this educational diversity, over 65 % of all participants reported being victims of cybercrime, a finding that both align with and diverges from prior studies.

Existing research indicates that the likelihood of falling victim to online fraud is influenced by several factors, among which educational attainment plays a significant role. Studies have demonstrated that individuals with lower levels of education are more susceptible to consumer fraud (Whitty, 2018). However, research also suggests a nuanced relationship between education level and fraud victimization. For instance, individuals at the extreme ends of educational attainment, such as those with no high school degree or graduate degree, are less likely to become victims of fraud (Schoepfer & Piquero, 2009), indicating a U-shaped pattern in this relationship.

Moreover, individuals who have completed higher education and spend more time online are found to be at greater risk of being targeted by fraudsters (Paek & Nalla, 2015). This association underscores the impact of routine online activities on victimization risk, highlighting the role of online interactions in cybercrime vulnerability. Additionally, older individuals, who typically have higher levels of education, are identified as particularly vulnerable to cyber-fraud victimization (Whitty, 2019). This demographic often exhibits traits such as high impulsivity, engagement in risky online behaviors, and addictive tendencies, all of which heighten their susceptibility to online scams.

4.4. Cybercrime Victimization, Ideal Victims, and the North-South Divide

The outcomes of our investigation underscore the pervasive impact of cybercrime in Nigeria, with a notable majority of participants (65.20 %) reporting personal victimization experiences (Aborisade et al., 2024). This prevalence underscores the widespread nature of cybercrime and its substantial effect on the study population. Conversely, 33.40 % of respondents indicated no encounters with cybercrime incidents, revealing a subset of individuals within Nigeria unaffected by this criminal activity. This contrast initiates discussions surrounding ideal victimization and the interplay between the Global North and West Africa (Nigeria), a subject rarely explored in online fraud literature.

The operations of groups like the Yahoo Boys, originating in Nigeria but impacting globally, have garnered increased attention to victims of online fraud. However, existing research predominantly centers on victims from Western societies (Button et al., 2014, 2015; Cross, 2020; Drew & Webster, 2024) and some non-Western contexts like China (Tao, 2022; Wang, 2023), with limited studies dedicated to West African nations such as Nigeria (Aborisade et al., 2024). It is plausible that the unequal distribution of research attention on certain issues is due to the tendency of Western media to focus on high-profile victims from Western countries. Additionally, research funding often prioritizes Western-centric perspectives, resulting in a lack of attention and resources for other regions, including West African nations such as Nigeria (Mosbah-Natanson & Gingras, 2014). These biases perpetuate assumptions and inadvertently marginalize victims from non-Western contexts, thus highlighting the concept of «ideal victims» where certain victims may be considered more “ideal victims” than others. Online fraud victims in Western societies such as the United States, the United Kingdom, and Australia are no less significant than their counterparts in Nigeria.

Building upon Christie’s (1986) seminal work on ideal victims, which delineates the traits of an ideal victim, our study investigated the dynamics of online fraud

victimization within the Nigerian context. Christie (1986) posits that ideal victims are perceived to embody specific traits aligning with societal norms of innocence, vulnerability, and lack of culpability, eliciting positive societal reactions. This public response could potentially prevent crimes against potential victims or bring criminal actors to justice. Other scholars have utilized this concept to examine facets of cybercrime (Hock & Button, 2023; Loyens & Paraciani, 2023). Utilizing this concept, we explore not only the dynamics of scams targeting Nigerians but also global societal responses, including research funding allocations, to crimes affecting Nigerians as victims. We argue that power dynamics between the Global North and South, alongside the structure of the global economy, shape victim perception, with victims from the West perceived as more deserving of «ideal victim» status than Nigerians, thus influencing both regional and global responses to crimes perpetrated against Nigerians. Given the significant rise in online fraud victimization in Nigeria, for example, from 2019 to 2022, the issue is deeply concerning.

However, it is worth noting that the power dynamics and economic structures that shape victim perception are complex and multifaceted and should not be oversimplified or reduced to a single factor. Also, regional agencies and Nigerian authorities are primarily responsible for their citizens rather than shifting local responsibilities to external bodies and international communities (e.g., Western nations) to support victims of online fraud within Nigerian society. Finally, while online fraud victimization is indeed a serious issue in Nigeria, the phenomenon is not unique to the country and occurs in many other parts of the world as well.

Conclusion

Our study, derived from 896 participants, has presented insights into cybercrime victimization, focusing on gender disparities, socioeconomic factors, educational attainment's influence on online fraud vulnerability, and cybercrime victimization through the lens of ideal victimization juxtaposed with the North-South socioeconomic divide. Our analysis has highlighted gender differences in cybercrime victimization experiences, with a higher proportion of men experiencing negative consequences, aligning with prior research like Kadoya et al. (2021). We have offered fresh insights into this discourse, emphasizing the variability in gender disparities across contexts and the need for gender-sensitive approaches in addressing cybercrime. Secondly, our study has emphasized socioeconomic factors' pivotal role in cybercrime prevalence, particularly in Nigeria. The prevalence patterns of cybercrime incidents, especially E-Banking/ Payment-Card Fraud, have underscored socioeconomic dynamics in cybercrime perpetration in Nigeria, highlighting the centrality of the socioeconomic cybercrimes

category in Nigeria. Thirdly, we have shed light on the correlation between educational attainment and vulnerability to online fraud. While over 99 % of our participants were university-educated, the distribution across educational levels has varied, impacting susceptibility to cybercrime. Our findings align with existing research (Whitty, 2018), underscoring the nuanced relationship between education level and fraud victimization. Last but not least, considering the North-South socioeconomic divide, we have explored cybercrime victimization through the ideal victimization lens. Drawing upon Christie's (1986) ground-breaking work, we have delved into online fraud victimization dynamics within Nigeria, highlighting disparities in research attention and global responses to cybercrime affecting non-Western contexts. Our findings have emphasized the need for gender, inclusive, and contextual, sensitive approaches to cybercrime research and policymaking in Nigeria and beyond, given the global power dynamics discussed. These insights have informed the development of multidimensional and contextually sensitive approaches to address cybercrime and mitigate its impact on vulnerable populations worldwide.

References

- Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, 44(7), 1102–1120. <https://doi.org/10.1080/01639625.2022.2144779>
- Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, 3, 100044. <https://doi.org/10.1016/j.jeconc.2023.100044>
- Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, 34(1), 44–67. <https://doi.org/10.1525/jpms.2022.34.1.44>
- Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, 58(5), 1083–1097. <https://doi.org/10.1177/0022343320964549>
- Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, 61(1), 59–71. <https://doi.org/10.1177/00223433231214417>
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. <https://doi.org/10.1089/cyber.2010.0307>
- Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, 1, 100012. <https://doi.org/10.1016/j.jeconc.2023.100012>
- Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, 54(2), 193–211. <https://doi.org/10.1111/hojo.12123>
- Button, M., Nicholls, C. M., 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. <https://doi.org/10.1177/0004865814521224>
- Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, 64, 101675. <https://doi.org/10.1016/j.tele.2021.101675>
- Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2
- Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14

- Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, 55, 1–12. <https://doi.org/10.1016/j.ijlcj.2018.08.001>
- Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, 20(3), 358–375. <https://doi.org/10.1177/1748895819835910>
- De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 108, 106310. <https://doi.org/10.1016/j.chb.2020.106310>
- Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, 3, 100053. <https://doi.org/10.1016/j.jeconc.2024.100053>
- Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, 30(2), 88–99. <https://doi.org/10.1080/19393555.2020.1804647>
- Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2, 13–20. <https://doi.org/10.1007/s11416-006-0015-z>
- Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, 48(4), 437–457. <https://doi.org/10.1177/03091325241246015>
- Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, 35(6), 748–783. <https://doi.org/10.1177/10790632221082663>
- Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, 18(7), 1311–1334. <https://doi.org/10.1080/15564886.2023.2186996>
- Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44–57. <https://doi.org/10.1016/j.ijlcj.2016.07.002>
- Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. <https://doi.org/10.1109/icccf.2016.7740439>
- Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10050983>
- Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10051047>
- Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10050896>
- Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10050994>
- Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.
- Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1(1), 1–6. <https://doi.org/10.5281/zenodo.18276>
- Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, 12(1), 1–8. <https://doi.org/10.5281/zenodo.1467308>
- Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, 12, 649565. <https://doi.org/10.3389/fpsyg.2021.649565>
- Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, 10(3), 146. <https://doi.org/10.3390/rel10030146>
- Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. <https://doi.org/10.1080/01639625.2024.2352049>
- Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, 25(8), 504–511. <https://doi.org/10.1089/cyber.2021.0332>

- Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14–26. <https://doi.org/10.1016/j.tele.2019.04.009>
- Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals (“Yahoo Boys”) and Politicians (“Yahoo men”). *Heliyon*, 8(11), e11142. <https://doi.org/10.1016/j.heliyon.2022.e11142>
- Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, 61(3), 381–398. <https://doi.org/10.1111/hojo.12485>
- Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, 2, 100033. <https://doi.org/10.1016/j.jeconc.2023.100033>
- Loyens, K., & Paraciani, R. (2023). Who is the (“Ideal”) Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors’ Discretion. *The Sociological Quarterly*, 64(1), 27–45. <https://doi.org/10.1080/00380253.2021.1974321>
- Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, 61(1), 72–86. <https://doi.org/10.1177/00223433231220264>
- Mba, G., Onalapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). <https://doi.org/10.1145/3041021.3053892>
- McGerty, L. J. (2000). «Nobody lives only in cyberspace»: Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, 3(5), 895–899. <https://doi.org/10.1089/10949310050191863>
- Meikle, W., & Cross, C. (2024). “What action should I take?”: Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, 3, 100054. <https://doi.org/10.1016/j.jeconc.2024.100054>
- Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, 14(1), 300–315. <https://doi.org/10.5281/zenodo.3755848>
- Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, 62(5), 626–646. <https://doi.org/10.1177/0011392113498866>
- Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, 28(1), 96–112. <https://doi.org/10.1007/s12119-023-10100-3>
- Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, 25, 173–191. <https://doi.org/10.1007/s12117-020-09397-5>
- Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimization and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, 29, 283–301. <https://doi.org/10.1007/s10610-021-09497-0>
- Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimization: a Systematic Review. *Journal of Police and Criminal Psychology*, 34, 231–245. <https://doi.org/10.1007/s11896-019-09334-5>
- Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, 13(2). <https://doi.org/10.5281/zenodo.3702333>
- 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.
- Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, 6(1), 55. <https://doi.org/10.31920/2516-2713/2023/6n1a4>
- Ojolo, T., & Adewumi, S. A. (2020). Understanding youths’ perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, 9(4), 243. <https://doi.org/10.31920/2634-3622/2020/v9n4a11>
- Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, 36(2), 350–372. <https://doi.org/10.1057/s41284-022-00342-5>
- Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: ‘Yahoo’Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, 9(2), 003.

- Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, 43(4), 626–642. <https://doi.org/10.1016/j.ijlcj.2015.02.003>
- Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. <https://doi.org/10.4324/9781315205786>
- Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, 31, 208–225. <https://doi.org/10.1057/s41284-017-0095-0>
- Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, 37(2), 209–215. <https://doi.org/10.1016/j.jcrimjus.2009.02.003>
- Tade, O., & Adeniyi, O. (2017). ‘They withdrew all I was worth’: Automated teller machine fraud and victims’ life chances in Nigeria. *International Review of Victimology*, 23(3), 313–324. <https://doi.org/10.1177/0269758017704330>
- Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. *Media, Culture & Society*, 44(6), 1199–1214. <https://doi.org/10.1177/01634437221088952>
- Timofeyev, Y., & Dremova, O. (2022). Insurers’ responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, 68, 100520. <https://doi.org/10.1016/j.ijlcj.2021.100520>
- Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, 0(0). <https://doi.org/10.1177/00111287231158571>
- Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, 49(1), 145–181. <https://doi.org/10.1007/s12103-022-09706-4>
- Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, 43(1), 17–34. <https://doi.org/10.1108/PIJPSM-07-2019-0122>
- Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, 3, 100052. <https://doi.org/10.1016/j.jeconc.2024.100052>
- Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, 21(2), 105–109. <https://doi.org/10.1089/cyber.2016.0729>
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292. <https://doi.org/10.1108/jfc-10-2017-0095>

Authors information



Aminu Muhammad Auwal – Bachelor of Science in Information Technology, IT Specialist, University of Jos
Address: PMB 2084, Jos, Plateau State, Nigeria
E-mail: i.elameenu@gmail.com
ORCID ID: <https://orcid.org/0009-0005-1799-7876>
WoS Researcher ID: <https://www.webofscience.com/wos/author/record/JFS-7098-2023>
Google Scholar ID: <https://scholar.google.com/citations?user=RDxPEr4AAAAJ>



Suleman Lazarus – PhD in Cybercrime and Criminology, Visiting Fellow at the Mannheim Centre for Criminology, London School of Economics and Political Science; Fellow at the Centre of Excellence on Ageing, University of Surrey; Honorary Lecturer at the Centre for Cybercrime and Economic Crime, University of Portsmouth.
Address: Houghton Street, London, WC2A 2AE, United Kingdom; Stag Hill, Guildford, GU2 7XH, United Kingdom; St. George's Building, Portsmouth, PO1 2HY, United Kingdom.
E-mail: suleman.lazarus@gmail.com
ORCID ID: <https://orcid.org/0000-0003-1721-8519>
Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57205679641>
WoS Researcher ID: <https://www.webofscience.com/wos/author/record/629543>
Google Scholar ID: <https://scholar.google.com/citations?user=Em8EXqcAAAAJ>

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – May 16, 2024

Date of approval – May 28, 2024

Date of acceptance – December 13, 2024

Date of online placement – December 20, 2024



Научная статья

УДК 34:004:343.9:004.8

EDN: <https://elibrary.ru/jvglrh>

DOI: <https://doi.org/10.21202/jdtl.2024.44>

Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности

Амину Мухаммад Аувал

Университет Джоса, Джос, Нигерия

Сулеман Лазарус 

Лондонская школа экономики и политических наук, Лондон, Великобритания

Университет Суррея, Гилфорд, Великобритания

Портсмутский университет, Портсмут, Великобритания

Ключевые слова


виктимизация,
виктимология,
жертва киберпреступления,
киберкриминология,
киберпреступность,
кибершпионаж,
онлайн-мошенничество,
правовая политика,
цифровая криминология,
цифровые технологии

Аннотация

Цель: выявление основных проблем виктимизации в результате роста киберпреступности в мире в целом и в нигерийском обществе в частности с позиций социологических подходов и с помощью трехчастной концепции киберпреступности (Tripartite Cybercrime Framework, TCF), состоящей из геополитических, психосоциальных и социально-экономических категорий киберпреступности.

Методы: основу методологии составили социологический метод исследования. Процесс сбора данных включал распространение опросника среди 896 участников из академической среды, в том числе студентов и сотрудников университета, и анализ ответов респондентов. Представленные данные анализировались с помощью описательной статистики, особое внимание при этом было уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к онлайн-мошенничеству и виктимизации в результате киберпреступлений через призму концепции идеальной жертвы и социально-экономического разрыва между Севером и Югом.

Результаты: в статье представлен анализ трехчастной концепции киберпреступности. На основе изучения данных, полученных в ходе анкетирования, установлено, что 65,20% участников опроса когда-либо становились жертвами киберпреступников. Выявлен гендерный перекося среди жертв киберпреступлений в сторону мужчин (64,69%).

 Корреспондирующий автор

© Аувал А. М., Лазарус С., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Установлены закономерности в распределении киберпреступлений. Все киберпреступления против опрошенных лиц относились к категории социально-экономических, что подчеркивает распространенность киберпреступности и актуальность противодействия ей в нигерийском социуме. Особое внимание уделено вопросам гендерного неравенства, социально-экономическим факторам, влиянию уровня образования на уязвимость к киберпреступлениям. Проблема виктимизации рассмотрена с точки зрения концепции идеальной жертвы. **Результаты** исследования позволяют получить представление о распространенности и распределении конкретных видов киберпреступности социально-экономической категории среди исследуемой группы населения.

Научная новизна: в исследовании впервые используется подход трехчастной концепции киберпреступности (TCF) для изучения виктимизации в результате киберпреступлений в нигерийском обществе. Новизна представленного исследования обусловлена еще и тем, что сложившиеся на глобальном Севере концептуальные основы противодействия киберпреступности не вполне применимы в Нигерии.

Практическая значимость: полученные результаты демонстрируют необходимость применения тщательно выверенных гендерных, инклюзивных и контекстуальных подходов к разработке национальной правовой политики борьбы с киберпреступностью, могут быть положены в обоснование разрабатываемых правотворческих решений в области предупреждения и противодействия проявлениям киберпреступности, а также в основу правовых мер защиты жертв киберпреступлений.

Для цитирования

Аувал, А. М., Лазарус, С. (2024). Социолого-криминологическое исследование проблем виктимизации: предварительный этап и новая область категоризации киберпреступности. *Journal of Digital Technologies and Law*, 2(4), 915–942. <https://doi.org/10.21202/jdtl.2024.44>

Список литературы

- Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, 44(7), 1102–1120. <https://doi.org/10.1080/01639625.2022.2144779>
- Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, 3, 100044. <https://doi.org/10.1016/j.jeconc.2023.100044>
- Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *Journal of Popular Music Studies*, 34(1), 44–67. <https://doi.org/10.1525/jpms.2022.34.1.44>
- Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research*, 58(5), 1083–1097. <https://doi.org/10.1177/0022343320964549>
- Akoto, W. (2024). Who spies on whom? Unravelling the puzzle of state-sponsored cyber economic espionage. *Journal of Peace Research*, 61(1), 59–71. <https://doi.org/10.1177/00223433231214417>
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. <https://doi.org/10.1089/cyber.2010.0307>
- Button, M., Hock, B., Shepherd, D., & Gilmour, P. (2023). Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology*, 1, 100012. <https://doi.org/10.1016/j.jeconc.2023.100012>

- Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2015). Online Fraud Victims in England and Wales: Victims' Views on Sentencing and the Opportunity for Restorative Justice? *The Howard Journal of Criminal Justice*, 54(2), 193–211. <https://doi.org/10.1111/hojo.12123>
- Button, M., Nicholls, C. M., 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. <https://doi.org/10.1177/0004865814521224>
- Button, M., Blackburn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, 64, 101675. <https://doi.org/10.1016/j.tele.2021.101675>
- Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08305-3_2
- Cross, C. (2018a). Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp. 261–280). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65021-0_14
- Cross, C. (2018b). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, 55, 1–12. <https://doi.org/10.1016/j.ijlcrj.2018.08.001>
- Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, 20(3), 358–375. <https://doi.org/10.1177/1748895819835910>
- De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 108, 106310. <https://doi.org/10.1016/j.chb.2020.106310>
- Drew, J. M., & Webster, J. (2024). The victimology of online fraud: A focus on romance fraud victimisation. *Journal of Economic Criminology*, 3, 100053. <https://doi.org/10.1016/j.jeconc.2024.100053>
- Genc, Y., Kour, H., Arslan, H. T., & Chen, L. C. (2021). Understanding Nigerian e-mail scams: A computational content analysis approach. *Information Security Journal: A Global Perspective*, 30(2), 88–99. <https://doi.org/10.1080/19393555.2020.1804647>
- Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2, 13–20. <https://doi.org/10.1007/s11416-006-0015-z>
- Hall, T., & Yarwood, R. (2024). New geographies of crime? Cybercrime, southern criminology and diversifying research agendas. *Progress in Human Geography*, 48(4), 437–457. <https://doi.org/10.1177/03091325241246015>
- Harper, C. A., Smith, L., Leach, J., Daruwala, N. A., & Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, 35(6), 748–783. <https://doi.org/10.1177/10790632221082663>
- Hock, B., & Button, M. (2023). Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*, 18(7), 1311–1334. <https://doi.org/10.1080/15564886.2023.2186996>
- Ibrahim, S. (2016a). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44–57. <https://doi.org/10.1016/j.ijlcrj.2016.07.002>
- Ibrahim, S. (2016b). Causes of socioeconomic cybercrime in Nigeria. In *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada (pp. 1–9). IEEE. <https://doi.org/10.1109/icccf.2016.7740439>
- Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 191–198). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10050983>
- Idem, U. J., & Olarinde, E. S. (2023). Cybercrime and its Negative Effects on Youth's Development, the Economy and Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 199–204). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10051047>
- Idem, U. J., Olarinde, E. S., Anwana, E. O., Ogundele, A. T., Awodiran, M. A., & Omomen, M. A. (2023a). The Prosecution of Cybercrimes in Nigeria: Challenges and Prospects. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 178–183). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10050896>
- Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023b). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 184–190). IEEE. <https://doi.org/10.1109/cymaen57228.2023.10050994>

- Jaishankar, K. (2011). Introduction: Expanding Cyber Criminology with an Avant-Garde Anthology. In *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (pp. xxvii–xxxv). Boca Raton: CRC Press.
- Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1(1), 1–6. <https://doi.org/10.5281/zenodo.18276>
- Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology*, 12(1), 1–8. <https://doi.org/10.5281/zenodo.1467308>
- Kadoya, Y., Khan, M. S. R., Narumoto, J., & Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. *Frontiers in Psychology*, 12, 649565. <https://doi.org/10.3389/fpsyg.2021.649565>
- Lazarus, S. (2019). Where is the Money? The Intersectionality of the Spirit World and the Acquisition of Wealth. *Religions*, 10(3), 146. <https://doi.org/10.3390/rel10030146>
- Lazarus, S. (2024). Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the «Black Axe» Confraternity. *Deviant Behavior*, 1–25. <https://doi.org/10.1080/01639625.2024.2352049>
- Lazarus, S., & Button, M. (2022). Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide. *Cyberpsychology, Behavior, and Social Networking*, 25(8), 504–511. <https://doi.org/10.1089/cyber.2021.0332>
- Lazarus, S., & Okolorie, G. U. (2019). The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents. *Telematics and Informatics*, 40, 14–26. <https://doi.org/10.1016/j.tele.2019.04.009>
- Lazarus, S., Button, M., & Adogame, A. (2022a). Advantageous Comparison: Using Twitter Responses to Understand Similarities between Cybercriminals (“Yahoo Boys”) and Politicians (“Yahoo men”). *Heliyon*, 8(11), e11142. <https://doi.org/10.1016/j.heliyon.2022.e11142>
- Lazarus, S., Button, M., & Kapend, R. (2022b). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, 61(3), 381–398. <https://doi.org/10.1111/hojo.12485>
- Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023). Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps. *Journal of Economic Criminology*, 2, 100033. <https://doi.org/10.1016/j.jeconc.2023.100033>
- Loyens, K., & Paraciani, R. (2023). Who is the (“Ideal”) Victim of Labor Exploitation? Two Qualitative Vignette Studies on Labor Inspectors’ Discretion. *The Sociological Quarterly*, 64(1), 27–45. <https://doi.org/10.1080/00380253.2021.1974321>
- Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, 61(1), 72–86. <https://doi.org/10.1177/00223433231220264>
- Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1301–1310). <https://doi.org/10.1145/3041021.3053892>
- McGerty, L. J. (2000). «Nobody lives only in cyberspace»: Gendered subjectivities and domestic use of the Internet. *CyberPsychology & Behavior*, 3(5), 895–899. <https://doi.org/10.1089/10949310050191863>
- Meikle, W., & Cross, C. (2024). “What action should I take?»: Help-seeking behaviours of those targeted by romance fraud. *Journal of Economic Criminology*, 3, 100054. <https://doi.org/10.1016/j.jeconc.2024.100054>
- Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, 14(1), 300–315. <https://doi.org/10.5281/zenodo.3755848>
- Mosbah-Natanson, S., & Gingras, Y. (2014). The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). *Current Sociology*, 62(5), 626–646. <https://doi.org/10.1177/0011392113498866>
- Murça, A., Cunha, O., & Almeida, T. C. (2024). Prevalence and Impact of Revenge Pornography on a Sample of Portuguese Women. *Sexuality & Culture*, 28(1), 96–112. <https://doi.org/10.1007/s12119-023-10100-3>
- Musotto, R., & Wall, D. S. (2020). More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*, 25, 173–191. <https://doi.org/10.1007/s12117-020-09397-5>
- Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, 29, 283–301. <https://doi.org/10.1007/s10610-021-09497-0>
- Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, 34, 231–245. <https://doi.org/10.1007/s11896-019-09334-5>

- Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, 13(2). <https://doi.org/10.5281/zenodo.3702333>
- 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.
- Ojolo, T. L., & Singh, S. B. (2023). Interrogating the Yahoo-Yahoo Menace: An Analysis of Moral Decadence, Poverty, and Unemployment In Nigeria. *Journal of African Films and Diaspora Studies*, 6(1), 55. <https://doi.org/10.31920/2516-2713/2023/6n1a4>
- Ojolo, T., & Adewumi, S. A. (2020). Understanding youths' perception and factors advancing cybercrime (yahoo-yahoo) in Ado-Ekiti, Ekiti State, Nigeria. *African Journal of Gender, Society & Development*, 9(4), 243. <https://doi.org/10.31920/2634-3622/2020/v9n4a11>
- Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, 36(2), 350–372. <https://doi.org/10.1057/s41284-022-00342-5>
- Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money: 'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *Global Journal of Interdisciplinary Social Sciences*, 9(2), 003.
- Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, 43(4), 626–642. <https://doi.org/10.1016/j.ijlcrj.2015.02.003>
- Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and justice in digital society*. New Delhi: Routledge. <https://doi.org/10.4324/9781315205786>
- Rich, T. (2018). You can trust me: A multimethod analysis of the Nigerian email scam. *Security Journal*, 31, 208–225. <https://doi.org/10.1057/s41284-017-0095-0>
- Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, 37(2), 209–215. <https://doi.org/10.1016/j.jcrimjus.2009.02.003>
- Tade, O., & Adeniyi, O. (2017). 'They withdrew all I was worth': Automated teller machine fraud and victims' life chances in Nigeria. *International Review of Victimology*, 23(3), 313–324. <https://doi.org/10.1177/0269758017704330>
- Tao, H. (2022). Loving strangers, avoiding risks: Online dating practices and scams among Chinese lesbian (lala) women. *Media, Culture & Society*, 44(6), 1199–1214. <https://doi.org/10.1177/01634437221088952>
- Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: evidence from Russia. *International Journal of Law, Crime and Justice*, 68, 100520. <https://doi.org/10.1016/j.ijlcrj.2021.100520>
- Wang, F. (2023). Sentencing Disparity and Focal Concern: An Assessment of Judicial Decisions on Sha Zhu Pan Cases Collected From China Judgements Online. *Crime & Delinquency*, 0(0). <https://doi.org/10.1177/00111287231158571>
- Wang, F., & Topalli, V. (2024). Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *American Journal of Criminal Justice*, 49(1), 145–181. <https://doi.org/10.1007/s12103-022-09706-4>
- Weijer van de, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*, 43(1), 17–34. <https://doi.org/10.1108/PIJPSM-07-2019-0122>
- Whittaker, J. M., Lazarus, S., & Corcoran, T. (2024). Are fraud victims nothing more than animals? Critiquing the propagation of "pig butchering" (Sha Zhu Pan, 杀猪盘). *Journal of Economic Criminology*, 3, 100052. <https://doi.org/10.1016/j.jeconc.2024.100052>
- Whitty, M. (2018). Do you love me? Psychological characteristics of Romance scam victims. *Cyberpsychology Behavior and Social Networking*, 21(2), 105–109. <https://doi.org/10.1089/cyber.2016.0729>
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292. <https://doi.org/10.1108/jfc-10-2017-0095>

Сведения об авторах



Амину Мухаммад Аувал – бакалавр в области информационных технологий, специалист в области информационных технологий, Университет Джоса

Адрес: Нигерия, PMB 2084, штат Плато, г. Джос

E-mail: i.elameenu@gmail.com

ORCID ID: <https://orcid.org/0009-0005-1799-7876>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/JFS-7098-2023>

Google Scholar ID: <https://scholar.google.com/citations?user=RDxPEr4AAAAJ>



Сулеман Лазарус – PhD в области киберпреступности и криминологии, приглашенный специалист Центра криминологии им. Маннхайма, Лондонская школа экономики и политических наук; сотрудник Центра изучения старения населения, университет Суррея; почетный преподаватель Центра по изучению киберпреступности и экономической преступности, Портсмутский университет

Адрес: Великобритания, WC2A 2AE, г. Лондон, Хьютон Стрит; Великобритания GU2 7XH, г. Гилфорд, Стэг Хилл; Великобритания, PO1 2HY, г. Портсмут, Сент-Джордж Билдинг.

E-mail: suleman.lazarus@gmail.com

ORCID ID: <https://orcid.org/0000-0003-1721-8519>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57205679641>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/629543>

Google Scholar ID: <https://scholar.google.com/citations?user=Em8EXqcAAAAJ>

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.27.41 / Сделки

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 16 мая 2024 г.

Дата одобрения после рецензирования – 28 мая 2024 г.

Дата принятия к опубликованию – 13 декабря 2024 г.

Дата онлайн-размещения – 20 декабря 2024 г.