Discover Psychology

RESEARCH Open Access

Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria

Aminu Muhammad Auwal[1] and Suleman Lazarus[2,3*]

*Correspondence:
Suleman Lazarus
suleman.lazarus@gmail.com
[1]Faculty of Natural Sciences, University of Jos, Jos, Plateau State, Nigeria
[2]Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), Houghton Street, London WC2A 2AE, UK
[3]Department of Sociology, University of the Western Cape, Cape Town, South Africa

Abstract

Despite much cybercrime originating in Nigeria, little is known about national victims compared to international victims of these crimes. In this study, we utilise the results from a survey of 1034 university staff and students to assess their experiences of victimisation using the Tripartite Cybercrime Framework (TCF). This framework distinguishes between socio-economic, geopolitical, and psychosocial forms of cybercrime. The analysis revealed a gender distribution skewed toward males (64.9%) and a notable predominance of Master's students. Among participants who reported cybercrime victimisation (65.4%), all incidents were classified under the socio-economic category. This pattern highlights the dominance of financially motivated cybercrime in the Nigerian context. These offences, listed in descending order of prevalence, include e-banking and payment-card fraud (58.6%), identity theft (11.1%), job scams (10.9%), cryptocurrency scams (10.6%), non-delivery scams (4.8%), and phishing attacks (4.0%). Alongside these TCF-related findings, our data indicate that among affected individuals, 354 men (52.4%) and 322 women (47.6%) reported negative consequences. In the full sample, 64.9% were male and 35.1% were female. However, only 38.7% of victims reported their incidents to authorities, and 14.9% received any form of restitution. This study builds on preliminary findings by pioneering the use of the Tripartite Cybercrime Framework with a larger, more diverse quantitative dataset to provide valuable insights into global research gaps and response disparities.

1 Introduction

Although Nigerian-based cybercriminals have gained widespread notoriety for their online scams around the globe [1–3], the plight of their local victims remains largely ignored. While Nigeria has gained a global reputation as a hub for internet scams targeting individuals worldwide [1, 2], research on victims within Nigerian society is almost non-existent. According to the World Cybercrime Index, Nigeria ranks as the leading country in West Africa for cybercrime and is positioned fifth globally [1]. Nigeria is a critical focus for studying regional victimisation patterns due to its significant role in global cybercrime. As a result, the UK Home Office commissioned a qualitative study to shed further light on cybercrime practices in West African countries, specifically Nigeria, as areas with a high risk of fraud aimed at Western nations [3]. Cybercrime

operations in the region are highly sophisticated in terms of technical skill, operational impact, and cash-out mechanisms. Perpetrators are colloquially referred to as "Yahoo Boys" [3, 4]. Yahoo Boys engage in diverse forms of fraud, such as romance fraud, advance fee fraud and cryptocurrency scams [3, 4].

Cybercrime is a global phenomenon [3]. This highlights the importance of understanding the impact of cybercrime in Nigeria, as its prevalence increases [5, 6]. While many scholars have explored cybercrime victimisation in various contexts [7–14], limited research has focused on victims in Nigeria. This represents an important gap that limits understanding of how cybercrime victimisation manifests locally, especially given the growing prominence of Nigerian cybercrime syndicates.

Existing studies have primarily relied on qualitative methods to explore cybercrime victimisation. For instance, Aborisade et al. [15] employed interpretative phenomenological analysis through semi-structured video interviews with ten victims of Nigerian romance fraudsters from six different nations. Although this study highlighted the global reach of Nigerian cybercriminals, it did not address the experiences of Nigerian victims. Similarly, Tade and Adeniyi [16] used in-depth interviews with ATM fraud victims, revealing the emotional trauma and reliance on social support networks post-victimisation. Neither of these studies could draw on quantitative data to investigate demographic characteristics and patterns of cybercrime victimisation.

We, therefore, resolved to address both issues by pursuing a quantitative approach to measure the extent and nature of cybercrime victimisation within a specific context. This strategy allows us to identify patterns and trends, which give a more comprehensive account of victims' characteristics and the prevalence of cybercrime incidents. By these means, we offer a broader understanding of cybercrime's impact on Nigerian society and provide empirical evidence to inform both academic discourse and practical interventions. By focusing on a largely under-researched population, this study aims to contribute to the global understanding of cybercrime victimisation while accounting for the unique sociocultural dynamics of Nigeria. To address these gaps and aims, this study is guided by the following research questions:

1. What is the prevalence and nature of cybercrime victimisation among university staff and students in Nigeria, including demographic patterns?
2. To what extent are the victimisation experiences of Nigerian victims consistent with the socio-economic category of the Tripartite Cybercrime Framework (TCF)?

2 Literature review

2.1 The concept of cybercrime

The concept of "cybercrime" encompasses unlawful activities conducted via the Internet and Information and Communication Technology (ICT), including "cyber-dependent" and "cyber-enabled crimes" [2, 5, 17–20]. Cyber-dependent crime refers to crimes that can only be committed using computer systems or networks, such as hacking, malware distribution, and denial-of-service attacks. These crimes are inherently tied to the digital environment and cannot occur without access to technology. On the other hand, cyber-enabled crime refers to traditional crimes facilitated or enhanced by digital technology, such as online fraud, identity theft, and cyberstalking. These crimes are not inherently dependent on technology but use it as a tool to commit the offence.

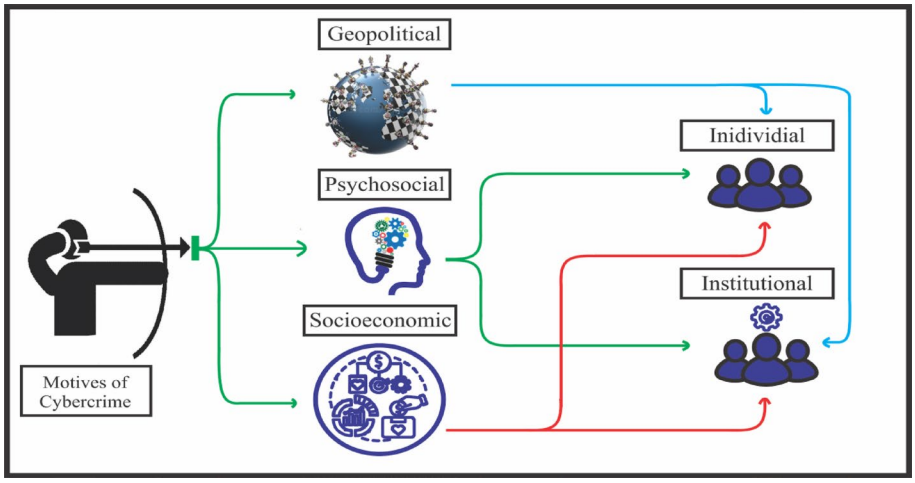

Fig. 1 Tripartite cybercrime framework (TCF)

Table 1 The tripartite cybercrime framework (TCF) motivational groups

Cybercrime type	Definition	Primary motivations	Examples
Socio-economic	Financially motivated cybercrime driven by deception, manipulation, and fraud.	Monetary or economic gain	Non-delivery fraud, cryptocurrency scams, business email compromise, romance scams.
Psychosocial	Cybercrimes driven by psychological motivations aimed at causing emotional distress or harm.	Psychological dominance or control; causing distress	Cyberstalking, cyberbullying, online harassment, revenge porn.
Geopolitical	Politically motivated cybercrimes with national or international implications.	Political or ideological influence; control over security	Cyber espionage, state-sponsored malware attack, infrastructure sabotage, disinformation and election interference.

It is common for security agencies, researchers, and the media to group various digital offenses under "cybercrime," ignoring their unique attributes, as Lazarus [21] noted. However, we consider the distinction a useful one as it highlights the importance of networks for cyber-enabled crimes, the focus of our study. The conflation of "cyber-enabled crimes" [22] and "people-centric cybercrimes" [23] makes it difficult to differentiate financially motivated crimes like "online fraud" from psychologically motivated ones like "revenge pornography" (e.g. [2, 21]). We now utilise the Tripartite Cybercrime Framework (TCF) [2, 21] to contribute to ongoing discussions on online fraud victimisation.

2.2 Tripartite cybercrime framework (TCF)

Non-empirical works (e.g. [24]) and empirical studies (e.g. [11, 25]) have studied cybercrime using the Tripartite Cybercrime Framework (TCF), as detailed in Fig. 1; Table 1. Ibrahim [2] argues that while cybercrimes in Nigeria are primarily financially driven, not all cyber-enabled crimes, such as revenge pornography, share this attribute. Drawing from these classifications, we highlight the unique characteristics of cybercrimes in Nigeria.

However, these tripartite categories are not rigidly defined, and instances of overlap often occur. For example, hacktivists may release stolen personal information to convey political messages, demonstrating both psychological and geopolitical implications.

Despite such overlaps, the TCF remains a valuable tool for identifying and categorising the distinct characteristics of various cybercrime types in Nigeria and beyond. Nonetheless, as Ibrahim [2] proposed, the application of the TCF in Nigeria highlights significant gaps in the documentation of certain cybercrime types. For instance, cyber espionage (geopolitical) and revenge porn (psychosocial), which are more prevalent in countries like Belgium, Canada, and the United Kingdom, are underrepresented in Nigerian contexts [2]. To address whether the framework does indeed apply in Nigeria warrants closer examination. Specific features of the context which merit attention are the distinct socioeconomic pressures shaping cybercrime involvement but also the limited documentation and unique contextual factors that differentiate Nigerian cybercrime from its Global North counterparts. It is worthy, therefore, to adapt cybercrime frameworks to reflect regional dynamics and realities.

2.3 The social life of digital crime in Nigeria

There is some evidence on various aspects of cybercrime prosecution, regulation, and its impact on Nigeria from existing conference papers [26–28]. Idem et al. [26] identify key challenges hindering cybercrime prosecution, including inadequate legislation, ineffective law enforcement, slow legal processes, and limited forensic capabilities. Building on this, Idem et al. [27] stress the urgent need for reform within regulatory agencies to mitigate Nigeria's status as a top country for cybercrime growth. Similarly, Idem [28] highlights the significant role of Nigeria's Cybercrimes Law in deterring cybercrime, safeguarding online businesses, and promoting internet enterprises. Together, these studies highlight the multifaceted challenges posed by cybercrime in Nigeria and underscore the need for legislative, regulatory, and socio-economic interventions.

Several studies illuminate the normalisation of cybercrime within Nigerian society. For instance, research reports such as [29] and [30] highlight economic instability, corruption, and peer influence as significant drivers of its prevalence. Similarly, scholars have emphasised the influence of political corruption, peer pressure, financial hardship, and inadequate social support systems [31–33]. Research has drawn parallels between internet scammers ("Yahoo Boys") and corrupt politicians ("Yahoo Men"), underlining the pervasive nature of corruption in both cybercrime and politics [4]. Many Nigerians live in abject poverty, while public fund embezzlement by politicians remains widespread [2, 4]. Additionally, some academic investigations, such as [34] and [35] highlight the lucrative nature of cybercrime and the complicity of corrupt law enforcement officers, asserting that financial incentives intersect with institutional vulnerabilities to sustain illicit online practices. Notably, incidents of cybercrime have increased significantly in recent years. Hence, cybercrime in Nigeria can be regarded as a multifaceted phenomenon rooted in socio-economic disparities, institutional deficiencies, and cultural influences.

The rise of economic cybercrime in Nigeria has become a growing concern for various stakeholders. Idem and Olarinde [6] examined its negative effects on youth development, the economy, and governance, identifying unemployment, poverty, corruption, and ineffective governance as key drivers of youth involvement in cybercriminal activities. They also provide recommendations to address these issues. Analysis of cybercrime and cybersecurity incident reports by the Economic and Financial Crimes Commission (EFCC) from 2019 to 2022 reveals a sharp rise in online fraud. Figure 2 summarises this trend.

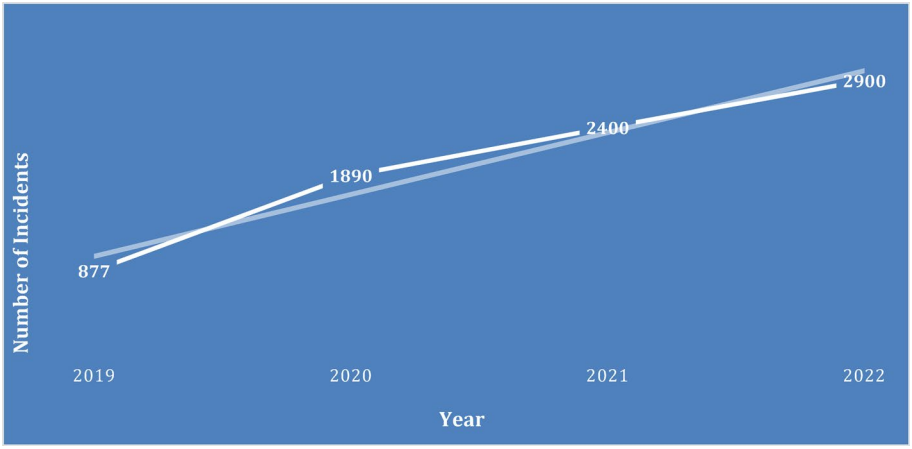

Fig. 2 The rise of reported online fraud incidents by victims

Figure 2 reveals a 115% increase from 2019 to 2020, a 173% rise by 2021, and a projected 231% increase in 2022. These figures, however, only reflect reported cases, as many incidents go unreported.

In other words, Fig. 2 illustrates a significant escalation in reported cybercrime incidents over the 4-year period from 2019 to 2022. The Economic and Financial Crimes Commission (EFCC) witnessed a substantial surge in reported cybercrime incidents during this timeframe. In 2019, 877 reported incidents increased to 1890 in 2020, a rise of approximately 115% from the previous year. By 2021, incidents further rose to 2400, marking an increase of about 173% compared to 2019. In 2022, reported incidents reached 2900, an approximate 231% increase from the baseline in 2019. These statistics highlight the exponential growth of online scams and underscore the urgent need for scholarly inquiry into victimisation patterns within the country. This marked surge in cybercrime activities, substantiated by the escalating number of convictions reported by the EFCC, spotlights a significant uptick in cybercrime within Nigeria. This trend is emblematic of the activities of cybercriminal entities, predominantly recognised as Yahoo Boys (cf [3, 36–38]).

2.4 Research on victim experiences

The actions of Yahoo Boys have global repercussions, prompting increased research on victims of online fraud. However, most studies on cybercrime victimisation focus on Western societies and Asian nations like China [7–9, 13, 39–42]. In contrast, research on victimisation in African nations like Nigeria is relatively scarce, with only a few studies, such as Mba et al. [43] and Tade and Adeniyi [16], addressing this context. This imbalance may stem from Western media's focus on victims from their own countries and the priorities of research funding allocations, which inadvertently marginalise victims from Nigeria. This study highlights the severe harm Yahoo Boys inflict on local citizens in Nigeria, a reality often overshadowed by the extensive focus on victims beyond national boundaries. By shedding light on the experiences of victims in Nigeria, we aim to challenge the prevailing Western-centric narrative and emphasise the universality of the issue (as stated above). We endeavour to contribute to a deeper understanding of online fraud and its impact on victims worldwide.

2.5 The role of Yahoo Boys in Nigerian digital crime

Several qualitative studies have explored the diverse facets of Nigerian cybercriminals by examining self-proclaimed offenders [35, 37, 38], convicted individuals within Nigeria [44], and those convicted abroad [45]. Empirical literature consistently indicates that men are the primary perpetrators of cybercrime in Nigeria, coordinating socio-economic digital crimes on the internet. The dominant discourse on Nigerian cybercrime tends to centre on male perpetrators (e.g., [35, 38]). This pattern is not necessarily due to an exclusive analytical focus on them but rather a reflection of their greater participation in cybercrime activity [4]. Ogunleye et al. [37] offer a contrasting perspective by examining female participation. Their study reveals that boyfriends or brothers, often mentor self-proclaimed female cybercriminals. Like their male counterparts, economic hardship and necessity are central to their criminal conduct, supporting the prevalence and relevance of socio-economic cybercrime in this region (see Fig. 1; Table 1).

As outlined in Ibrahim [2], the TCF categorises cybercrime motivations into three domains: socio-economic, psychosocial, and geopolitical. The present study examines the experiences of individual victims of Yahoo Boys in Nigeria, whose victimisation is overwhelmingly tied to socio-economic motivations (i.e., financial gain). By design, this study excluded items that capture psychosocial motivations (e.g., thrill-seeking or status-driven offending) or geopolitical cybercrime, which typically involve state actors, corporations, or critical infrastructure, rather than interpersonal fraud targeting individuals. The absence of these categories in our findings reflects the scope and sample design rather than their broader irrelevance. Despite these insights into offender characteristics, few studies have investigated the experiences of cybercrime victims in Nigeria, with notable exceptions being [43] and [16].

2.6 Alignment and variation in earlier work

Numerous studies have produced convergent findings using various data sources, enhancing the credibility of empirical research on cybercrime issues in Nigeria. These studies include interviews with frontline law enforcement officers [36], analysis of scam emails [46, 47], examination of music lyrics [30, 33], interviews with Nigerian parents [48, 49], interviews with online fraudsters [35, 37, 38], analysis of tweets [4, 50], and victims' perceptions and experiences in Ghana [51]. Although cybercrime experiences in Ghana may initially seem a local issue, research shows that cybercrime offenders often migrate from Nigeria to Ghana [52]. The consistency among these studies reaffirms a fundamental understanding of the characteristics of online offenders and the types of cybercrimes they commit. Additionally, non-empirical studies [26, 27] support these findings, consolidating evidence from diverse research methodologies. However, there remains a paucity of research on cybercrime victims in Nigeria, with only a few studies, such as Mba et al. [43] and Tade and Adeniyi [16], addressing this area.

Although a small number of studies have investigated cybercrime victims in Nigeria [16, 43], they have not employed quantitative approaches to explore respondents' demographic characteristics and experiences of cybercrime. Building on this gap, our preliminary analysis of a smaller participant group (see "Pilot Study and Questionnaire Design" section) revealed early indications of a high prevalence of socio-economic cybercrime among university populations. This initial insight reinforced the need to reassess how victim experiences are documented and understood. For example, Mba et

al. [43] combined data from a Nigerian online forum with web searches to locate additional scam posts of a similar nature. Additionally, Hall and Ziemer [25], focusing on Armenia, used the Tripartite Cybercrime Framework (TCF) as a reference point, and De Kimpe et al. [53] drew on the Tripartite Cybercrime Framework (TCF) to guide the focus of their research on Belgium. Similarly, Lazarus, Button and Kapend's [11] study in the United Kingdom adopted the Tripartite Cybercrime Framework (TCF) as a conceptual lens. However, no studies have examined cybercrime in Nigeria through the lens of the TCF. We aim to address this gap by examining cybercrime victimisation in Nigeria through the classifications provided by the TCF. We utilise the TCF, "The Socioeconomic Theory of Nigerian Cybercriminals," proposed by Ibrahim [2], as a framework for our research. By employing quantitative methods and focusing on the Nigerian context, this study seeks to contribute novel insights into the patterns of cybercrime victimisation and expand the application of the TCF to new geographical and cultural settings.

3 Methods and materials

We employed a distributed survey approach to collect data from a diverse cohort of students, and staff. The sampling frame consisted of individuals affiliated with the University of Jos, Nigeria, which served as the primary research site. Our questionnaire explores the Tripartite Cybercrime Framework, which categorises cybercrime into socio-economic, 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 gain a deeper understanding of their experiences with cybercrime. While participants' responses were anonymised and kept confidential, ethical approval (Ref: NS/2024/0186) was obtained from the University of Jos, Nigeria, to ensure adherence to academic and research guidelines. All research activities involving human participants adhered to the National Code of Health Research Ethics (NCHRE) of the National Health Research Ethics Committee of Nigeria (NHREC).

Data collection occurred in two phases: the first, between June and August 2023, and the second, from December 2024 to January 2025, to broaden the participant pool. We opted for the traditional pen-and-paper questionnaire method for data collection. In contrast to computer-aided approaches, this method eliminates the necessity for participants to utilise their smartphone data. This decision was informed by economic and infrastructural realities in Nigeria, where financial constraints make mobile data usage for voluntary surveys an unlikely priority, unlike other countries where completing an online survey is effectively costless. Many Nigerians in legitimate employment struggle to provide for themselves and their dependents, making any additional costs a challenge. Additionally, political corruption, rampant embezzlement, and mismanagement of public funds contribute to financial instability, making individuals more reluctant to expend personal resources on research participation [2, 4, 50]. It is also commonplace for university workers to experience delayed salary payments, and many students face financial hardship, which in some cases pushes them towards Yahoo Boys' activities as an alternative means of survival [2, 50]. Consequently, we considered the potential disincentive posed by the need to use or purchase mobile data and opted for a method that would encourage broader participation.

3.1 Pilot study and questionnaire design

We conducted a pilot study to:

1. Determine the feasibility of the research methodology,
2. Ensure that the questionnaire was adequately formulated and easy to understand and.
3. The draft questionnaire can be distributed to a small sample of students and staff at the University of Jos, Nigeria, to gather all the required data.

After assessing the feasibility and validity of the questionnaire, we proceeded with distributing it to a broader group of participants. The operationalisation of key measures was carefully considered in the questionnaire design. Cybercrime victimisation was assessed through direct questions about participants' experiences with various forms of cyber fraud, including financial scams, phishing, and identity theft. To clarify how these categories were defined and operationalised in the survey, see Table 2. To measure 'underreporting of incidents', respondents were asked whether they reported cybercrime experiences, the reasons for their decision, and the perceived effectiveness of reporting mechanisms. 'Effectiveness of remedial measures' was examined through questions on access to legal or institutional support following cybercrime victimisation, including whether they sought assistance and the outcomes of such efforts. A summary of the questionnaire instrument, including all sections and operational definitions of key cybercrime categories, is provided in Appendix A.

A research team member, a university professional, provided participants with a concise oral overview of the study in classroom and office settings, ensuring they understood its purpose before seeking their informed consent. They were also informed that participation was entirely voluntary, with no incentives or penalties attached. Participants were instructed to complete the distributed questionnaire at their convenience and return it to a designated box within the university if they agreed to participate. A total of 1034[1] participants completed the questionnaire (as shown in Tables 3 and 4). The survey was meticulously designed and distributed through structured channels to ensure efficiency and broad reach. Before participating, participants provided informed

Table 2 Types of cybercrime and operational definitions

Type of cybercrime	Operational definition / examples
E-banking / payment-card fraud	Unauthorized access to or manipulation of online bank accounts or payment cards to steal funds. Includes ATM skimming, fraudulent online transfers, and unauthorized credit/debit card use.
Identity theft	Illicit acquisition and use of another individual's personal or financial information (e.g., name, SSN, BVN, passwords) to impersonate them for financial gain or other fraudulent activities.
Job scams	Fake employment offers that deceive victims into paying upfront fees or sharing sensitive personal information under false pretenses.
Crypto scams	Fraudulent cryptocurrency investment or trading platforms promising high returns but designed to steal funds or data.
Non-Delivery Scams	Fraudulent sales where victims pay for goods or services that are never delivered.
Phishing	Deceptive emails, messages, or websites used to trick victims into revealing confidential data (e.g., passwords, PINs).

[1] Of the 1034 participants, 896 were initially recruited and analysed. An additional 138 participants were subsequently included, prompting a re-analysis of the dataset. The preliminary analysis (n = 896) was released as a preprint (e.g. [54]), though it did not undergo peer review.

Table 3 Sample demographics. Percentages are calculated based on the total sample size ($N = 1034$)

Category	Subcategory	Frequency (*N*)	Percentage (%)
Informed consent response	Yes	1034	98.19
	No	19	1.81 (not included in the final sample)
Gender	Male	671	64.91
	Female	363	35.09
Educational level	Undergraduate students	402	38.88
	Master's students	561	54.28
	Doctoral candidates	39	3.77
	Teachers/admin staff	32	3.07

Table 4 Cybercrime victimisation prevalence

Category	Subcategory	Frequency (*N*)	Percentage (%)
Cybercrime victimisation	Victims	676	65.38
	Non-victims	358	34.62
Gender breakdown of victims	Male victims	354	52.40
	Female victims	322	47.60
Type of cybercrime experienced	E-banking/payment-card fraud	396	58.58
	Identity theft	75	11.10
	Other forms of cybercrime (e.g., job scams, crypto scams, phishing)	205	30.32
Reporting behaviour	Reported cases	262	38.74
	Unreported cases	414	61.24
Restitution after reporting	Stolen money recovered	101	14.95
	No restitution received	575	85.06

Percentages are calculated based on the number of identified victims ($N = 676$)

consent, and stringent measures were implemented to safeguard their anonymity and confidentiality throughout the data collection process.

3.2 Data analysis

We conducted an analysis to identify the geographical clusters and sectors most affected by cybercrime. Using statistical methods, 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 were used to analyse the data, ensuring clarity and accessibility. Means and medians were computed using Excel spreadsheets to facilitate the calculation of relevant counts and percentages. While this method has its limitations, we offer the following justifications for this approach:

- *Exploratory analysis*: Descriptive statistics are valuable tools for conducting exploratory analysis. They enable researchers to gain an initial understanding of the data by summarising key characteristics such as central tendency and variability. Since this is a preliminary study, this approach enables the identification of basic patterns in cybercrime experiences among participants without assuming underlying relationships. Given the complex and context-specific sociocultural dynamics in Nigeria, and the exploratory nature of this study, it would be methodologically premature to test specific statistical relationships (e.g., between gender or

educational background and victimisation) and to calculate and interpret inferential statistics (e.g., p-values, confidence intervals, or effect sizes) without a larger and more representative sample. For these reasons, we opted to focus on descriptive analysis in this initial investigation.

- *Data presentation*: Descriptive statistics are essential for clearly and concisely presenting critical findings, making them accessible to a broad audience, including undergraduate students from diverse disciplines. Given that the study focuses on cybercrime experiences among university students and workers in Nigeria, descriptive statistics provide a straightforward way to communicate significant findings about the prevalence and characteristics of cybercrime in this population.
- *Simple data structures*: The survey instrument used in the study has a relatively simple structure, with well-defined variables and clear response categories. 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 at this stage and could introduce unnecessary complexity. Descriptive statistics are an efficient way to analyse and summarise data. They allow researchers to identify key trends and patterns without assuming underlying relationships. By presenting findings clearly and concisely, descriptive statistics make complex data more accessible. This approach provides valuable insights into the experiences of cybercrime victimisation among the study population.

4 Results

This section presents the findings from the quantitative analysis of 1034 responses, highlighting the frequencies and percentages associated with each category identified in the study, as summarised in Tables 3 and 4.

4.1 Participant gender distribution

The findings of this study reveal a notable gender disparity in cybercrime victimisation. While men represent a larger proportion of the sample (64.91%, $N = 671$), the distribution of victims is more balanced than expected. Out of the 676 victims, 354 were male (52% of male participants) and 322 were female (48% of female participants). This suggests that women are disproportionately affected by cybercrime relative to their representation in the sample. Specifically, women are slightly overrepresented among the victims, given that they make up only 35% of the total sample but represent 48% of the victims. These findings highlight the importance of considering gender dynamics in understanding and addressing cybercrime victimisation. The overrepresentation of women in the victim category calls for targeted, gender-sensitive strategies to address the specific vulnerabilities and needs of female victims while also acknowledging the impact on male victims.

4.2 Educational level

The sample included participants from a range of educational backgrounds: 38% were undergraduates, 54% were Master's students, 4% were doctoral candidates, and 3% were teachers and administrative staff. This diversity in educational levels ensures the sample's heterogeneity, enriching the study's insights and enhancing the generalisability of the findings. Importantly, this variety in educational background may also offer valuable

perspectives on how different levels of education influence experiences of cybercrime, helping to contextualise victimisation trends within various academic and professional groups. Further exploration of how educational levels intersect with cybercrime experiences could provide a deeper understanding of the factors contributing to vulnerability and response behaviours across different demographics.

4.3 Documented harm from cybercrime

A significant proportion of participants (65%) reported experiencing adverse cybercrime incidents, highlighting the pervasive impact of cybercrime on the study population. On the other hand, 35% of participants indicated they had not been affected by cybercrime, suggesting a subset of individuals who remain unaffected by this phenomenon.

4.4 Category of cybercrime

The analysis reveals distinct prevalence patterns in the types of cybercrime experienced. E-banking/Payment Card Fraud was the most common form of cybercrime, affecting about 59% of victims. Identity Theft accounted for about 11% of cases, while other forms, such as online job scams, represented about 30% of reported incidents. These findings provide important insights into the specific socio-economic types of cybercrime prevalent in the Nigerian context.

4.5 Reported incidents

The study found that 39% of participants reported cybercrime incidents to relevant authorities or entities, indicating a moderate engagement with reporting mechanisms. In contrast, the majority (61%) did not report any incidents, suggesting potential underreporting and areas for improvement in reporting practices.

4.6 Recovery of financial loss/follow-up action

Among participants who reported cybercrime incidents, only a minority (15%) indicated that stolen funds were reversed or appropriate actions were taken. The remaining (85%) reported no remedial actions, highlighting the challenges in achieving restitution or resolution following cybercrime victimisation. 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 endeavours. It also emphasises the need for improved response mechanisms to address cybercrime consequences effectively.

5 Discussion

We build upon insights garnered through a distributed survey approach, outlined in Tables 4 and 5, to advance understanding of cybercrime victimisation across diverse demographic spectra. Importantly, while some may contend that our data cannot be used to make sweeping generalisations about cybercrime in Nigeria, it nonetheless offers valuable insights into the lived realities of university populations, a key segment of Nigerian society that is both highly connected and increasingly targeted. The findings shed light on how socio-economic drivers manifest in digital victimisation patterns, providing a lens through which broader national trends can be critically examined. While this

Table 5 Thematic summary of key findings

Theme	Key finding	Description	Implications
1. High participation and consent	Strong willingness to engage	98.19% of participants provided informed consent, indicating a high level of engagement with the research process	Reflects the perceived relevance of cybercrime issues among the population; suggests public readiness to engage in dialogue and action on cybercrime
2. Educational diversity	Broad range of educational backgrounds	Sample included undergraduates (38.88%), master's students (54.28%), doctoral candidates (3.77%), and teachers/admin staff (3.07%)	Enhances the generalisability of findings; demonstrates that cybercrime cuts across various educational strata
3. Prevalence of cybercrime experiences	High incidence of victimisation	65.38% of participants reported having experienced some form of cybercrime	Establishes cybercrime as a prevalent threat; supports the case for urgent intervention by policymakers, educators, and digital safety advocates
4. Types of cybercrime encountered	Dominance of socio-economic offences	Most common forms included e-banking/payment-card fraud (58.58%), identity theft (11.10%), job scams (10.90%), cryptocurrency scams (10.60%), non-delivery scams (4.80%), and phishing (4.02%)	Indicates a predominance of financially motivated crimes; aligns with the socio-economic dimension of the Tripartite Cybercrime Framework; suggests focal points for prevention strategies
5. Underreporting of incidents	Low engagement with formal authorities	Only 38.74% of victims reported their experiences to authorities	Signals a lack of trust in law enforcement or perceived futility in reporting; highlights the need for improved and victim-friendly reporting pathways
6. Lack of remedial action	Minimal restitution for victims	Just 14.95% of those who reported incidents received any form of recovery or remedial action	Reveals shortcomings in institutional response and victim support; underscores the urgency for reform in justice mechanisms and post-victimisation care

section comprises six primary subsections listed below, we analyse relevant contours of cybercrime victimisation in our study.

1. The Sect. 5.1 examines disparities in cybercrime experiences based on gender, highlighting differences in fraud victimisation patterns between men and women.
2. The Sect. 5.2 analyses the pivotal role of socio-economic factors in cybercrime in Nigeria, particularly concerning financial motives and digital fraud schemes.
3. The Sect. 5.3 explores the correlation between educational attainment and vulnerability to online fraud, considering how awareness and digital literacy impact cybercrime victimisation.
4. The Sect. 5.4 investigates cybercrime victimisation through the lens of ideal victimisation, juxtaposed with the socioeconomic divide between the Global North and West Africa.
5. The Sect. 5.5 considers the Routine Activities Theory with socio-economic status as contributing factors in cybercrime victimisation and perpetration.
6. The Sect. 5.6 addresses key study constraints, including the sampling scope within a university setting, reliance on self-reported data, and potential issues related to generalisability.

5.1 Gender dimension of online fraud victimisation

Gender disparities in cybercrime victimisation are a central focus of our study, revealing notable differences in experiences between men and women. Our data analysis indicates that among individuals affected by cybercrime, 354 men (52.40%) and 322

women (47.60%) reported negative consequences. Furthermore, the overall distribution of cybercrime victims shows that 64.91% are male and 35.09% are female. The gender distribution among victims appears nearly even, despite differences in overall sample proportions. These findings somewhat highlight a gendered pattern in cybercrime victimisation, with a higher proportion of men experiencing negative consequences compared to women. This stresses the importance of adopting 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 emphasises the significance of considering gender dynamics in understanding and responding to cybercrime phenomena.

Our study's analysis of gender disparities in cybercrime victimisation both aligns with and diverges from findings in prior research. For example, a study in the United Kingdom [11] asserts that while women tend to perceive psychosocial cybercrimes, such as revenge pornography, as more severe than men, no discernible gender disparities exist in socioeconomic 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 socio-economic cybercrime victimisation, contributing to the discourse. Moreover, numerous studies have explored the intricate dynamics of cybercrime victimisation, shedding light on various influencing factors (e.g. [55, 56]). For example, research in Japan by Kadoya et al. [56] identified gender and marital status as potential determinants of victimisation, indicating that males and married individuals are more susceptible to fictitious billing fraud. Although our study did not specifically inquire about marital status, our findings resonate with those of Kadoya et al. [56], corroborating the significance of gender in cybercrime victimisation.

The variability in gender disparities across different contexts is further illuminated by studies conducted in Finland [55] and the Netherlands [57]. 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 [55, 57]. Consequently, it is plausible to assert that the gender differences identified in our study may be attributed, in part, to disparities in crime reporting behaviour. This underscores the multifaceted nature of cyber victimisation reporting, often leading to cybercrimes being reported to organisations 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 [58]. Although our study did not investigate psychological traits and their association with online fraud victimisation, 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 victimisation, with other factors such as fraudster motivation and target vulnerability exerting considerable influence as well.

5.2 The centrality of socio-economic cybercrime

The findings of this study highlight the predominance of socio-economic cybercrime among the types reported by participants. As detailed in Table 5, e-banking/payment card fraud (58.58%) emerged as the most prevalent form, followed by identity theft (11.10%) and other fraudulent schemes (30.32%), including online job scams (10.90%),

cryptocurrency scams (10.60%), non-delivery scams (4.80%), and phishing (4.02%). These trends reinforce the centrality of socio-economics in cybercrime issues in Nigeria [2]. Financial motivations drive cybercriminal activities and reflect the broader socio-economic situation and dimension of Nigerian society [2–4].

This pattern aligns with the socio-economic category of the Tripartite Cybercrime Framework (TCF), which identifies economic deprivation and financial aspirations as key catalysts for cybercriminal behaviour. The prevalence and dominance of socio-economic cybercrime targeting financial transactions and identity fraud further reinforce the role of economic incentives in shaping cybercrime operations. Cybercriminals strategically exploit vulnerabilities in digital financial systems, employing deceptive tactics to target individuals seeking employment, investment opportunities, or online financial transactions.

Our research further highlights the clear prevalence of trends in cybercrime incidents, with e-banking/payment card fraud as the most dominant type, comprising 58.58% of reported cases. Identity theft accounts for 11.10%, while various other scams, including online job scams and phishing, collectively represent 30.32% of cases. All these offences fall within the socio-economic category of cybercrime, reinforcing the notion that cybercrime exhibits core characteristics across different regions, shaping human behaviour within specific local contexts (e.g. [5, 50]). The Tripartite Cybercrime Framework (TCF) delineates cybercrimes into three principal motivational components: socio-economic, psychological, and geopolitical, underlining the distinction between socio-economic and psychosocial cyber offences (e.g. [2, 11, 21]). Understanding these distinctions provides a more structured approach to analysing cybercrime victimisation.

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 [2]. Different nations' geopolitical and sociocultural contexts significantly shape their cyberspace behaviour. For instance, while revenge pornography is prevalent in Western countries like Portugal [10], the United Kingdom, Canada, etc [59], it may not be as pronounced in Nigeria. Furthermore, unlike Nigeria, countries such as the United States, Russia, China, and the United Kingdom face significant challenges with nation-sponsored cyber espionage (e.g. [60, 61]). These social and contextual nuances challenge the notion of cyberspace and physical space as distinct entities with clear boundaries, as highlighted by Ibrahim [2], and Jaishankar [18]. As a result, the conceptual frameworks commonly utilised in "the Global North" may not entirely apply in Nigeria, representing Africa south of the Sahara ([2], p. 55). 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 socio-economic 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 prioritises socio-economic cybercrime types, such as online scams. This emphasis is evident in the exclusive focus on financial crimes reported by the Economic and Financial Crimes Commission (EFCC) [4, 50], the elite enforcement agency in West Africa [36]. The lack of documentation could also stem from other factors, such as limited resources or inadequate infrastructure for detecting

and reporting these types of cybercrime. Furthermore, while sociocultural and geopolitical contexts influence cyberspace behaviour, it is essential to acknowledge that geopolitical cybercrime types often do not affect ordinary citizens, such as 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.

5.3 Educational attainment and online fraud victimisation

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, 38.88% were undergraduates, 54.28% were master's students, 3.77% were pursuing doctoral degrees, and 3.07% were educators and admin staff. Despite this educational diversity, over 65% of all participants reported being victims of cybercrime, a finding that both aligns with and diverges from prior studies.

Existing research suggests that the likelihood of falling victim to online fraud is influenced by several factors, with educational attainment playing a significant role. Studies have demonstrated that individuals with lower levels of education are more susceptible to consumer fraud (e.g. [62]).

However, research also suggests a nuanced relationship between education level and fraud victimisation. 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 [63], indicating a U-shaped pattern in this relationship. Moreover, individuals with higher education who spend more time online are found to be at greater risk of being targeted by fraudsters [64]. This association underlines the impact of routine online activities on victimisation risk, highlighting how increased online interactions contribute to cybercrime vulnerability. This demographic often exhibits traits such as high impulsivity, engagement in risky online behaviours, and addictive tendencies, all of which heighten their susceptibility to online scams. Similarly, Barth et al. [65] argue that the privacy valuations and reported online behaviours of experts are similar to those of lay users. Even with their advanced technical skills and clear grasp of privacy threats, many experts still take minimal precautions online. This suggests that even individuals with advanced knowledge are not immune to cybercrime risks, reinforcing the importance of cybersecurity awareness across all user groups.

5.4 Ideal victims of cybercrime, and the global north-south divide

The outcomes of our investigation underscore the pervasive impact of cybercrime in Nigeria, with a notable majority of participants (65.38%) reporting personal victimisation experiences (e.g. [15]). This stark reality not only highlights the widespread reach of cybercrime but also necessitates a deeper interrogation into the socio-economic and systemic factors that facilitate victimisation in the region. Furthermore, these findings suggest a layered victim experience within Nigeria that contrasts sharply with global narratives dominated by Western perspectives. Consequently, they prompt critical discussions on ideal victimisation and the interplay between the Global North and West Africa (Nigeria), a subject rarely addressed in online fraud literature.

The operations of groups like the Yahoo Boys, originating in Nigeria but impacting victims globally, have drawn significant attention. However, existing research

predominantly focuses on victims from Western societies [7, 8, 13, 14] and, to a lesser extent, non-Western contexts, such as China (e.g. [9, 41]). In contrast, limited attention has been devoted to West African nations, such as Nigeria (e.g. [16, 43]), resulting in a critical gap in understanding regional victimisation dynamics. Funding disparities exacerbate this imbalance; researchers (e.g. [66, 67]), note that only a fraction of global research funds is allocated to African contexts, despite the disproportionate impacts experienced in these regions.Historical legacies have significantly hindered the acknowledgement of scholastic contributions from non-Western nations, while Western academic endeavours continue to receive disproportionate visibility (e.g. [66–69]). These disparities are rooted in the uneven global distribution of academic power and resources, which perpetuates hierarchies that marginalise Global South scholars [66–68]. Citations, far from being neutral, function as instruments of academic gatekeeping, either reinforcing epistemic inequality or disrupting it by legitimising underrepresented voices [68]. Since citation metrics dictate future research trajectories, a paradigm shift is needed (e.g. [66–68]) -one that moves beyond traditional metrics and interrogates the biases that perpetuate Western academic dominance.

The unequal distribution of research attention on cybercrime issues can be attributed to the far-reaching influence of Western media compared to that of West Africa. Western media often prioritise high-profile victims within their own communities, predominantly from Western countries, over victims from West Africa. This media focus, coupled with mismatched funding priorities, highlights systemic inequalities that hinder the study of non-Western victims and exacerbate global disparities.

Additionally, there is a broader neglect of cross-border research. This lack of focus limits our understanding of how cybercriminal activities, including those originating from Nigeria, affect victims across multiple regions. To bridge this gap, a more inclusive research agenda is needed, one that examines victimisation beyond national and regional silos. Such an approach would ensure that the experiences of victims in West Africa are integrated into the global discourse on cybercrime.

As a result, these disparities in media representation and research funding perpetuate a narrow understanding of cybercrime victimisation, focusing primarily on Nigerian offenders while overlooking the nuanced realities faced by local victims. A shift towards more cross-border, comparative research approaches is necessary for a deeper understanding of cybercrime victimisation. Such an approach would provide a more nuanced and comprehensive analysis, highlighting the complexities often overlooked in existing studies. It would also disrupt dominant narratives that portray cybercrime through a limited lens, prioritising offenders over the experiences of West African victims.

Due to the fact that cybercrime originating in Nigeria affects victims worldwide, the regional focus is exclusively on offenders at the expense of local victims within Nigeria. Media portrayals exacerbate this imbalance by emphasising stereotypes and biases that marginalise Nigerian victims. Such portrayals align with Christie's [70] concept of "ideal victims," where societal responses to victimisation are shaped by socio-political power dynamics. Victims from the Global North are often recognised as more deserving of sympathy and support than those from the Global South, highlighting a disparity in global responses to cybercrime. While fraud victims in Western nations like the United States, the United Kingdom, and Australia receive significant attention, their Nigerian counterparts remain largely overlooked despite enduring similar harms.

Building on Christie's [70] framework, our study examined the dynamics of online fraud victimisation in Nigeria. Ideal victims are expected to align with societal norms of innocence, vulnerability, and lack of culpability, eliciting positive societal reactions. In Nigeria, these norms are complicated by cultural stereotypes associating Nigerians with cybercrime, which diminishes the perceived innocence or victimhood of local fraud victims. This stigma not only limits societal sympathy but also hinders institutional and global responses to crimes affecting Nigerian victims. Perceptions of innocence and vulnerability differ between Western and Nigerian contexts, with Nigerian victims often unjustly linked to offenders due to national stereotypes. This disparity reduces the societal and policy-level support extended to Nigerian victims, reinforcing inequities in global and regional responses. Furthermore, these findings suggest a layered victim experience within Nigeria that contrasts sharply with global narratives dominated by Western perspectives.

Other scholars (e.g. [71, 72]) have applied Christie's framework to examine cybercrime victimisation. Our study expands this analysis by highlighting how power dynamics between the Global North and South, coupled with global economic structures, influence perceptions of victimhood. Western victims are often deemed more deserving of "ideal victim" status, which shapes both regional and international responses to cybercrime involving Nigerians. Moreover, the global networks of cybercrime originating in Nigeria have contributed to a narrative that prioritises offenders, overshadowing the plight of local victims.

The significant rise in online fraud victimisation in Nigeria, particularly from 2019 to 2022 (see Fig. 2), underscores the urgency of addressing this issue. However, the power dynamics and economic structures shaping victim perception are complex and multifaceted and should not be oversimplified. Also, regional agencies and Nigerian authorities are primarily responsible for their citizens rather than shifting local responsibilities to external bodies and international communities. Strengthening these local mechanisms of accountability is essential to addressing victimisation more effectively. Media portrayals further entrench these imbalances. Western media often depict Nigerian offenders, Yahoo Boys, with heightened interest [30] while neglecting local victims. Similarly, Nigerian media focuses on the criminal exploits of Yahoo Boys but rarely highlights the experiences of their victims, particularly their fellow Nigerian citizens.

This dichotomy reinforces global stereotypes that frame Nigerians predominantly as offenders, marginalising victims in public and policy discourses. Such portrayals not only distort the realities of cybercrime in Nigeria but also impede the development of comprehensive victim support frameworks. While online fraud victimisation is a serious issue in Nigeria [43], it is not unique to the country. Yahoo Boys have victims in many parts of the world, particularly the United States [44, 76, 78]. We conclude that media attention must be more inclusive and grounded in richer empirical engagement, recognising cybercrime victimisation in West Africa as both a regional and global phenomenon. This approach should affirm the equal significance of victims from all regions, ensuring they receive the support they deserve. This broader recognition of cybercrime victimisation necessitates a deeper exploration of the structural and situational factors that shape both offending and victimisation patterns. Understanding the distinct roles of socio-economic conditions and opportunity structures is crucial in further developing the analysis. In this regard, we briefly consider Routine Activities Theory (RAT) to

examine how cybercriminal behaviour emerges within specific socio-economic contexts. While the Routine Activities Theory provides useful situational insights, the Tripartite Cybercrime Framework (TCF) remains the core analytical lens of this study; therefore, RAT is discussed only marginally to complement, rather than drive, our main findings.

5.5 Considering routine activities theory and socio-economic status

While opportunities drive cybercrime engagement, economic conditions influence who has access to these opportunities and how they are exploited. The relationship between socio-economic status (SES) and crime has been widely debated in criminological literature. Routine Activities Theory (RAT) posits that crime occurs when three key elements converge: a motivated offender, a suitable target, and the absence of capable guardianship [73–75]. This framework emphasises opportunities rather than socio-economic conditions as the primary driver of criminal behaviour. From this perspective, individuals with greater ICT knowledge, access to digital infrastructure, or social connections to cybercriminal networks may be more likely to engage in cybercrime, regardless of their SES. The predominance of university students as cybercrime perpetrators in Nigeria [44, 76, 78], along with the increasing sophistication of digital fraud tactics [30, 36, 78], further supports this argument.

However, while RAT focuses on situational opportunities, SES remains a structural factor that indirectly influences criminal behaviour. Research on cybercrime in Nigeria suggests that economic constraints limit access to legitimate opportunities, pushing individuals to seek alternative financial survival, including illicit online activities [2, 50, 76–78]. In Africa south of the Sahara contexts (e.g., Nigeria, Ghana and Cameroon), where graduate unemployment is high and economic hardship is pervasive (e.g. [2–4, 78–80]). SES can shape individuals' exposure to cybercrime-enabling environments. Although SES does not directly cause online crime, it can increase the likelihood of individuals encountering and exploiting illicit opportunities. Since this study was conducted within a university setting, where participants were primarily students and staff, direct measurement of SES was not feasible. However, recognising the interplay between SES and opportunity structures remains essential in understanding the broader dynamics of cybercrime victimisation and perpetration.

5.6 Limitations

This study has limitations that should be acknowledged. First, the sampling scope was restricted to a university setting, with participants comprising only students and staff. While this provided valuable insights into cybercrime victimisation within an educated demographic, it limits the generalisability of findings to the broader body of Nigerian populations, including individuals outside academic institutions who may experience cybercrime differently. Second, participants' responses depended on their recollections of past cybercrime experiences, and some may have underreported or misrepresented their encounters due to stigma or concerns about confidentiality, particularly about romance fraud and hookup scams. Finally, the generalisability of the findings is constrained by the study's specific focus on a single university. The experiences of cybercrime victims may vary across different regions, economic backgrounds, and digital access levels. This highlights the importance of conducting additional research in diverse settings to reflect the full spectrum of cybercrime victimisation. Despite these

limitations, the study offers important insights into the overlooked experiences of local cybercrime victims and highlights key socio-economic dynamics that shape cybercriminal activities. Indeed, the study provides initial insights, and future research should draw on larger and more diverse samples across multiple regions to enhance external validity.

6 Conclusion

Drawing on responses from 1034 participants, this study provides key insights into cybercrime victimisation in Nigeria. It highlights gendered patterns, the central role of socio-economic factors, the influence of educational status on vulnerability, and broader global North–South disparities. Firstly, our analysis revealed notable gender differences in cybercrime victimisation experiences. Contrary to some prior research, we found a slightly higher proportion of men (52.40%) experiencing negative consequences compared to women (47.60%). This finding emphasises the need for gender-sensitive approaches in addressing cybercrime. Both men and women are significantly affected, and gender disparities may vary across different contexts.

Secondly, the study underscored the pivotal role of socio-economic factors in the prevalence of cybercrime in Nigeria. The dominance of E-Banking/Payment Card Fraud, accounting for 58.58% of reported incidents, highlights the centrality of socio-economic cybercrimes in the Nigerian context. This prevalence reflects underlying socio-economic dynamics and suggests that financial motives are a primary driver of cybercriminal activities in the region.

Thirdly, we examined the correlation between educational attainment and vulnerability to online fraud. Despite over 98% of our participants being university-educated, the distribution across different educational levels influenced susceptibility to cybercrime. This finding aligns with existing research (e.g., see "Educational attainment and online fraud victimisation" section), which suggests that advanced or expert knowledge does not necessarily confer immunity against cyber fraud. It highlights the need for comprehensive cyber awareness programmes targeting individuals at all educational levels. Also, this study's findings largely reinforce the patterns identified in our preliminary analysis [54, 81], particularly the dominance of socio-economic cybercrime experiences. Our updated sample (n = 1034) includes a greater number of undergraduate students and reflects increased institutional diversity. This broader base reveals more pronounced gender differences and clearer disparities in reporting and restitution, trends that were less evident in the earlier, more homogeneous dataset.

Moreover, considering the North–South socio-economic divide, we explored cybercrime victimisation through the lens of the "ideal victim" concept [70]. Our study highlights disparities in research attention and global responses to cybercrime, particularly the tendency of media and academic publications to focus predominantly on Western victims of Nigerian cybercriminals ("Yahoo Boys") while often overlooking victims within Nigeria itself. This bias contributes to a skewed global narrative that marginalises non-Western victims and overlooks the domestic impact of cybercrime in countries like Nigeria.

Our findings emphasise the necessity for inclusive and context-sensitive approaches to cybercrime research and policymaking. Global power dynamics shape both knowledge production and vulnerability to harm. It is therefore imperative to address the needs of all victims, regardless of geographical location. In academia, recognition and citation

are not mere formalities, because they sustain visibility, credibility, and participation in scholarly discourse [68]. Similarly, in the context of cybercrime discourse, we must develop multidimensional strategies. These must account for systemic inequities if we are to meaningfully mitigate the impact on vulnerable populations worldwide.

Certainly, this study contributes to a deeper understanding of cybercrime victimisation in Nigeria, challenging prevailing narratives that prioritise Western experiences. Context operates as a critical analytic resource in the production of understanding. In other words, understanding is never context-free; it relies on context as the scaffolding for interpretation. By highlighting the experiences of Nigerian victims, we call for greater international attention and resources to be directed towards addressing cybercrime in non-Western contexts.

Future research should expand the sampling scope, incorporate mixed-method approaches, and examine cybercrime victimisation across different social and economic groups to enhance the depth and applicability of findings. Recommendations for future research should also include further exploration of these dynamics, ensuring that cybercrime prevention and intervention strategies are equitable and globally inclusive. Additionally, this study recommends developing policies that focus on comprehensive education, targeted awareness campaigns, and gender-sensitive responses to mitigate cybercrime victimisation in both Western and non-Western contexts. We also call for a dual-pronged approach to cybercrime prevention. This should focus not only on reducing opportunities through digital security measures but also on addressing the underlying socio-economic conditions that facilitate engagement in online fraud. Furthermore, meeting the needs of the most vulnerable, particularly in countries like Nigeria, will necessitate sustained collaboration. Global, national, and local stakeholders must work together to create effective, context-specific solutions.

6.1 Policy and practical implications

Beyond contributing to academic understanding, these findings have direct implications for policy and institutional practice. Universities should implement targeted digital literacy programmes and awareness campaigns to help students recognise and respond to fraudulent schemes. Partnerships between higher education institutions, digital safety agencies, and law enforcement could facilitate the sharing of intelligence on emerging cybercrime tactics and provide accessible support services for victims. At a national level, law enforcement and regulatory bodies should prioritise preventive and educational strategies alongside punitive measures, recognising that many victims lack awareness rather than acting negligently. Embedding these measures within university policies and national cyber-safety frameworks can help mitigate the prevalence and impact of socio-economic cybercrime, while ensuring that responses are inclusive and sensitive to gender and contextual differences.

Supplementary Information

The online version contains supplementary material available at https://doi.org/10.1007/s44202-025-00479-5.

Supplementary Material 1

Acknowledgements
We thank Professor Lucinda Platt (London School of Economics and Political Science) for her insightful feedback on the initial draft of this article.

Author contributions
A.M.A. contributed to methodology, data curation, formal analysis, investigation, and writing – original draft.S.L. led the conceptualisation, contributed to methodology, and investigation, and was responsible for writing – original draft, writing – review & editing, and supervision. Both authors reviewed and approved the final manuscript and agree to be accountable for its content.

Funding
This work received no financial support from any funding agency, commercial entity, or not-for-profit sector.

Data availability
Data supporting the findings of this study are available from the corresponding author, subject to a reasonable request.

Declarations

Ethics approval and consent to participate
The primary Ethics approval for this study was obtained from the following institution: University of Jos, Nigeria. All procedures involving human participants were carried out in accordance with the National Code of Health Research Ethics (NCHRE) as issued by the National Health Research Ethics Committee of Nigeria (NHREC). Informed consent was obtained from all participants before they took part in the survey. Participation was voluntary, and respondents were informed about the study's purpose, confidentiality measures, and their right to withdraw at any time without consequences.

Consent for publication
Not applicable.

Competing interests
The authors declare no conflict of interest.

Received: 25 July 2025 / Accepted: 10 October 2025
Published online: 19 November 2025

References

1. Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F, Jan N. Mapping the global geography of cybercrime with the world cybercrime index. PLoS ONE. 2024;19(4):e0297312.
2. Ibrahim S. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. Int J Law Crime Justice. 2016;47:44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002.
3. Button M, Gilmour P, Hock B, Jain T, Jesperson S, Lazarus S, Pandey D, Sabia J. Scoping study on fraud centres: Ghana, India and Nigeria. Brighton: ITAD; 2024. https://www.itad.com/knowledge-product/scoping-study-on-fraud-centres-ghana-india-and-nigeria/.
4. Lazarus S, Button M, Adogame A. Advantageous comparison: using Twitter responses to understand similarities between cybercriminals ['yahoo boys'] and politicians ['yahoo men']. Heliyon. 2022;8(11):e11142. https://doi.org/10.1016/j.heliyon.2022.e11142.
5. Hall T, Yarwood R. New geographies of crime? Cybercrime, Southern criminology and diversifying research agendas. Prog Hum Geogr. 2024;48(4):437–57. https://doi.org/10.1177/03091325241246015.
6. Idem UJ, Olarinde ES. Cybercrime and its negative effects on youth's development, the economy and Nigeria. In: 2023 International conference on cyber management and engineering [CyMaEn]. 2023. pp. 199–204. https://doi.org/10.1109/cymaen57228.2023.10051047.
7. Cross C. Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims. Criminol Crim Just. 2019;20(3):358–75. https://doi.org/10.1177/1748895819835910.
8. Drew JM, Webster J. The victimology of online fraud: a focus on romance fraud victimisation. J Econ Criminol. 2024;3:100053. https://doi.org/10.1016/j.jeconc.2024.100053.
9. Wang F. Sentencing disparity and focal concern: an assessment of judicial decisions on Sha Zhu Pan cases collected from China judgements online. Crime Delinq. 2023. https://doi.org/10.1177/00111287231158571.
10. Murça A, Cunha O, Almeida TC. Prevalence and impact of revenge pornography on a sample of Portuguese women. Sex Cult. 2023;28(1):96–112. https://doi.org/10.1007/s12119-023-10100-3.
11. Lazarus S, Button M, Kapend R. Exploring the value of feminist theory in Understanding digital crimes: gender and cybercrime types. Howard J Crime Justice. 2022;61(3):381–98. https://doi.org/10.1111/hojo.12485.
12. Timofeyev Y, Dremova O. Insurers' responses to cyber crime: evidence from Russia. Int J Law Crime Justice. 2022;68:100520. https://doi.org/10.1016/j.ijlcj.2021.100520.
13. Button M, Nicholls CM, Kerr J, Owen R. Online frauds: learning from victims why they fall for these scams. Aust N Z J Criminol. 2014;47(3):391–408. https://doi.org/10.1177/0004865814521224.
14. Button M, Nicholls CM, Kerr J, Owen R. Online fraud victims in England and wales: victims' views on sentencing and the opportunity for restorative justice? Howard J Crim Justice. 2015;54(2):193–211. https://doi.org/10.1111/hojo.12123.
15. Aborisade RA, Ocheja A, Okuneye BA. Emotional and financial costs of online dating scam: a phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. J Econ Criminol. 2023;3:100044. https://doi.org/10.1016/j.jeconc.2023.100044.
16. Tade O, Adeniyi O. They withdrew all I was worth': automated teller machine fraud and victims' life chances in Nigeria. Int Rev Victimol. 2017;23(3):313–24. https://doi.org/10.1177/0269758017704330.
17. Button M, Hock B, Shepherd D, Gilmour P. Understanding the rise of fraud in England and Wales through field theory: blip or flip? J Econ Criminol. 2023;1:100012. https://doi.org/10.1016/j.jeconc.2023.100012.

18. Jaishankar K. Cyber criminology as an academic discipline: history, contribution and impact. Int J Cyber Criminol. 2018;12(1):1. https://doi.org/10.5281/zenodo.1467308.
19. Musotto R, Wall DS. More Amazon than mafia: analysing a DDoS stresser service as organised cybercrime. Trends Organ Crime. 2020;25(2):173–91. https://doi.org/10.1007/s12117-020-09397-5.
20. Loggen J, Moneva A, Leukfeldt R. A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. Comput Law Secur Rev. 2024;52:105858. https://doi.org/10.1016/j.clsr.2023.105858.
21. Lazarus S. Just married: the synergy between feminist criminology and the tripartite cybercrime framework. Int Soc Sci J. 2019;69(231):15–33. https://doi.org/10.1111/issj.12201.
22. McGuire M, Dowling S. Cybercrime: a review of the evidence. 2013. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
23. Gordon S, Ford R. On the definition and classification of cybercrime. J Comput Virol. 2006;2(1):13–20. https://doi.org/10.1007/s11416-006-0015-z.
24. Lazarus S, Tickner P, McGuire MR. Cybercrime against senior citizens: exploring ageism, ideal victimhood, and the pivotal role of socio-economics. Secur J. 2025. https://doi.org/10.1057/s41284-025-00482-4.
25. Hall T, Ziemer U. Online deviance in post-Soviet space: victimisation, perceptions and social attitudes amongst young people, an Armenian case study. Digit Geogr Soc. 2024;7:100096. https://doi.org/10.1016/j.diggeo.2024.100096.
26. Idem UJ et al. The prosecution of cybercrimes in Nigeria: challenges and prospects. In: 2023 International conference on cyber management and engineering [CyMaEn]. 2023. pp. 178–83. https://doi.org/10.1109/cymaen57228.2023.10050896.
27. Idem UJ et al. Cybercrime regulatory agencies need urgent reform to protect Nigeria. In: 2023 International conference on cyber management and engineering [CyMaEn]. 2023. pp. 184–90. https://doi.org/10.1109/cymaen57228.2023.10050994.
28. Idem UJ. 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]. 2023. pp. 191–8. https://doi.org/10.1109/cymaen57228.2023.10050983.
29. Ojolo T, Adewumi SA. Understanding youths' perception and factors advancing cybercrime [yahoo–yahoo] in Ado-Ekiti, Ekiti state, Nigeria. Afr J Gend Soc Dev. 2020;9(4):243–64. https://doi.org/10.31920/2634-3622/2020/v9n4a11.
30. Lazarus S, Olaigbe O, Adeduntan A, Dibiana ET, Okolorie GU. Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. J Econ Criminol. 2023;2:100033. https://doi.org/10.1016/j.jeconc.2023.100033.
31. Olaiya TA, Lamidi KO, Bello MA. Narrative of illicit money: 'yahoo' Boy [format] of cyber scams and governance challenges in Africa. Glob J Interdiscip Soc Sci. 2020;9(2):003. https://doi.org/10.35248/2155-6156.20.9.003.
32. Monsurat I. African insurance [spiritualism] and the success rate of cybercriminals in Nigeria: a study of the Yahoo Boys in Ilorin, Nigeria. Zenodo [CERN European Organization for Nuclear Research]. 2020. https://doi.org/10.5281/zenodo.3755848.
33. Adeduntan A. Rhyme, reason, rogue. J Pop Music Stud. 2022;34(1):44–67. https://doi.org/10.1525/jpms.2022.34.1.44.
34. Ojolo TL, Singh SB. Interrogating the yahoo–yahoo menace: an analysis of moral decadence, poverty, and unemployment in Nigeria. J Afr Films Diaspora Stud. 2023;6(1):55. https://doi.org/10.31920/2516-2713/2023/6n1a4.
35. Aransiola JO, Asindemade SO. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychol Behav Soc Netw. 2011;14(12):759–63. https://doi.org/10.1089/cyber.2010.0307.
36. Lazarus S, Okolorie GU. The bifurcation of the Nigerian cybercriminals: narratives of the economic and financial crimes commission [EFCC] agents. Telematics Inf. 2019;40:14–26. https://doi.org/10.1016/j.tele.2019.04.009.
37. Ogunleye YO, Ojedokun UA, Aderinto AA. Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in South-West Nigeria. Zenodo [CERN European Organization for Nuclear Research]. 2020. https://doi.org/10.5281/zenodo.3702333.
38. Ojedokun UA, Eraye MC. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int J Cyber Criminol. 2012;6(2):1001.
39. Meikle W, Cross C. What action should I take? help-seeking behaviours of those targeted by romance fraud. J Econ Criminol. 2024;3:100054. https://doi.org/10.1016/j.jeconc.2024.100054.
40. Cross C. Expectations vs. reality: responding to online fraud across the fraud justice network. Int J Law Crime Justice. 2018;55:1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001.
41. Tao H. Loving strangers, avoiding risks: online dating practices and scams among Chinese lesbian [lala] women. Media Cult Soc. 2022;44(6):1199–214. https://doi.org/10.1177/01634437221088952.
42. Wang F, Topalli V. Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. Am J Crim Justice. 2024;49(1):145–81. https://doi.org/10.1007/s12103-022-09706-4.
43. Mba G, Onaolapo J, Stringhini G, Cavallaro L. Flipping 419 cybercrime scams: targeting the weak and the vulnerable. In: Proceedings of the 26th international conference on the world wide web companion. 2017. pp. 1301–10. https://doi.org/10.1145/3041021.3053892.
44. Garba KH, Lazarus S, Button M. An assessment of convicted cryptocurrency fraudsters. Curr Issues Crim Just. 2024;36(1):1–17. https://doi.org/10.1080/10345329.2024.2403294.
45. Lazarus S. Cybercriminal networks and operational dynamics of business email compromise [BEC] scammers: insights from the 'black axe' confraternity. Deviant Behav. 2024;46(4):456–80. https://doi.org/10.1080/01639625.2024.2352049.
46. Genc Y, Kour H, Arslan HT, Chen L-C. Understanding Nigerian e-mail scams: a computational content analysis approach. Inf Secur J Glob Perspect. 2020;30(2):88–99. https://doi.org/10.1080/19393555.2020.1804647.
47. Rich T. You can trust me: a multimethod analysis of the Nigerian email scam. Secur J. 2018;31:208–25. https://doi.org/10.1057/s41284-017-0095-0.
48. Aborisade RA, Yahoo Boys. Yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. Deviant Behav. 2022;44(7):1102–20. https://doi.org/10.1080/01639625.2022.2144779.
49. Ibrahim S. Causes of socioeconomic cybercrime in Nigeria. Presented at IEEE international conference on cybercrime and computer forensic [ICCCF], Vancouver, BC, Canada. 2017. pp. 1–9. https://doi.org/10.1109/icccf.2016.7740439.
50. Lazarus S, Button M. Tweets and reactions: revealing the geographies of cybercrime perpetrators and the North-South divide. Cyberpsychol Behav Soc Netw. 2022;25(8):504–11. https://doi.org/10.1089/cyber.2021.0332.
51. Mensah RO, Mensah P, Opoku D. Experiences and perceptions of cybercrime victims in ghana: the perspective of digital consumers of agricultural produce. Cogent Educ. 2023;10(2):2285623. https://doi.org/10.1080/2331186X.2023.2285623.

52. Lazarus S, Button M, Garba KH, Soares AB, Hughes M. Strategic business movements? The migration of online romance fraudsters from Nigeria to Ghana. J Econ Criminol. 2025;7:100128. https://doi.org/10.1016/j.jeconc.2025.100128.
53. De Kimpe L, Ponnet K, Walrave M, Snaphaan T, Pauwels L, Hardyns W, Help. I need somebody: examining the antecedents of social support seeking among cybercrime victims. Comput Hum Behav. 2020;108:106310. https://doi.org/10.1016/j.chb.2020.106310.
54. Auwal AM. The overview of cybercrime and cyber security in Nigeria and its future trends. Res Sq. 2023. https://doi.org/10.21203/rs.3.rs-3307532/v2.
55. Näsi M, Danielsson P, Kaakinen M. Cybercrime victimisation and polyvictimisation in Finland—prevalence and risk factors. Eur J Crim Policy Res. 2021;29(2):283–301. https://doi.org/10.1007/s10610-021-09497-0.
56. Kadoya Y, Khan MSR, Narumoto J, Watanabe S. Who is next? A study on victims of financial fraud in Japan. Front Psychol. 2021;12:649565. https://doi.org/10.3389/fpsyg.2021.649565.
57. van de Weijer S, Leukfeldt R, Van der Zee S. Reporting cybercrime victimization: determinants, motives, and previous experiences. Polic Int J. 2020;43(1):17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122.
58. Norris G, Brookes A, Dowell D. The psychology of internet fraud victimisation: a systematic review. J Police Crim Psychol. 2019;34(3):231–45. https://doi.org/10.1007/s11896-019-09334-5.
59. Harper CA, Smith L, Leach J, Daruwala NA, Fido D. Development and validation of the beliefs about revenge pornography questionnaire. Sex Abuse. 2022;35(6):748–83. https://doi.org/10.1177/10790632221082663.
60. Akoto W. International trade and cyber conflict: decomposing the effect of trade on state-sponsored cyber attacks. J Peace Res. 2021;58(5):1083–97. https://doi.org/10.1177/0022343320964549.
61. Makridis C, Maschmeyer L, Smeets M. If it bleeps it leads? Media coverage on cyber conflict and misperception. J Peace Res. 2024;61(1):72–86. https://doi.org/10.1177/00223433231220264.
62. Titus RM, Gover AR. Personal fraud: the victims and the scams. In: Farrell G, Pease K, editors. Repeat victimisation: crime prevention studies. Volume 12. Monsey: Criminal Justice; 2001. pp. 133–51.
63. Schoepfer A, Piquero NL. Studying the correlates of fraud victimization and reporting. J Crim Justice. 2009;37(2):209–15. https://doi.org/10.1016/j.jcrimjus.2009.02.003.
64. Paek SY, Nalla MK. The relationship between receiving phishing attempt and identity theft victimization in South Korea. Int J Law Crime Justice. 2015;43(4):626–42. https://doi.org/10.1016/j.ijlcj.2015.02.003.
65. Barth S, De Jong MDT, Junger M. Lost in privacy? Online privacy from a cybersecurity expert perspective. Telematics Inf. 2022;68:101782. https://doi.org/10.1016/j.tele.2022.101782.
66. Mosbah-Natanson S, Gingras Y. The globalization of social sciences? Evidence from a quantitative analysis of 30 years of production, collaboration and citations in the social sciences (1980–2009). Curr Sociol. 2013;62(5):626–46. https://doi.org/10.1177/0011392113498866.
67. Mason S, Merga MK, Canché MSG, Roni SM. The internationality of published higher education scholarship: how do the 'top' journals compare? J Informet. 2021;15(2):101155. https://doi.org/10.1016/j.joi.2021.101155.
68. Lazarus S. An autoethnographic perspective on scholarly impact, citation politics, and north–south power dynamics. Life Writ. 2024. https://doi.org/10.1080/14484528.2024.2430666.
69. Collyer FM. Global patterns in the publishing of academic knowledge: global north, global South. Curr Sociol. 2018;66(1):56–73. https://doi.org/10.1177/0011392116680020.
70. Christie N. The ideal victim. London: Palgrave Macmillan UK; 1986. pp. 17–30.
71. Hock B, Button M. Non-Ideal victims or offenders? The curious case of pyramid scheme participants. Vict Offenders. 2023;18(7):1311–34. https://doi.org/10.1080/15564886.2023.2186996.
72. Loyens K, Paraciani R. Who is the ['ideal'] victim of labor exploitation? Two qualitative vignette studies on labor inspectors' discretion. Sociol Q. 2021;64(1):27–45. https://doi.org/10.1080/00380253.2021.1974321.
73. Cohen LE, Felson M. Social change and crime rate trends: a routine activity approach. Am Sociol Rev. 1979;44:588–608.
74. Akdemir N, Lawless CJ. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. Internet Res. 2020;30(6):1665–87. https://doi.org/10.1108/INTR-10-2019-0400.
75. Vakhitova ZI, Alston-Knox CL, Reynald DM, Townsley MK, Webster JL. Lifestyles and routine activities: do they enable different types of cyber abuse? Comput Hum Behav. 2019;101:225–37. https://doi.org/10.1016/j.chb.2019.07.012.
76. Soares AB, Lazarus S. Examining Fifty cases of convicted online romance fraud offenders. Crim Justice Stud. 2024;37(4):328–51. https://doi.org/10.1080/1478601X.2024.2429088.
77. Lazarus S, Soares AB. From business centres to hustle kingdoms: historical perspectives on innovative models of deviant education. Int Ann Criminol. 2025. https://doi.org/10.1017/cri.2025.1.
78. Soares AB, Lazarus S, Button M. Love, lies, and larceny: one hundred convicted case files of cybercriminals with Eighty involving online romance fraud. Deviant Behav. 2025. https://doi.org/10.1080/01639625.2025.2482824.
79. Whittaker JM, McGuire MR, Lazarus S. Conversations with deviant website developers: a case study of online shopping fraud enablers. J Criminol. 2025. https://doi.org/10.1177/26338076251321844.
80. Yushawu A, Jaishankar K. Sakawa in ghana: the influence of weak ties on economic cybercrime offender networks. Deviant Behav. 2025. https://doi.org/10.1080/01639625.2025.2459681.
81. Auwal AM, Lazarus S. Sociological and criminological research of victimization issues: preliminary stage and new sphere of cybercrime categorization. J Digi Technol Law. 2024;2(4):915–42.

Publisher's note