What Researchers Learned From 50 Cases Of Convicted Romance Scammers

A study examined 50 cases of convicted online romance fraudsters in Nigeria, offering a window into the scams orchestrated by the notorious "Yahoo Boys."

Conducted by researchers from Nigeria's Economic and Financial Crimes Commission (EFCC) and leading academic institutions, the investigation analyzed detailed case files to uncover patterns in victim targeting, technological preferences, and operational strategies.

Most Interesting Takeaways

1. **Demographics and Education**

The perpetrators were overwhelmingly male university students (74%), typically aged 18-26, revealing how cybercrime has become an alternative career path for educated but economically challenged young Nigerians.

2. **Technological Preferences**

Intriguingly, 58% of scammers preferred using Apple iPhones - a strategic choice suggesting they invest in high-end devices to project credibility and success to potential victims.

3. **Geographic Targeting**

A striking 56% of victims were from the United States, demonstrating how scammers strategically target regions perceived to have greater wealth and stronger online presence.

4. **Gender Dynamics**

The study revealed a pronounced gender disparity in victimization - 70% of scammers targeted female victims, suggesting a calculated exploitation of gender-specific vulnerabilities in online relationships.

5. **Platform Utilization**

Facebook emerged as the primary hunting ground, used in 46% of cases, followed by combined Facebook/Instagram usage, highlighting how mainstream social platforms become vectors for sophisticated fraud.

6. **Identity Deception Patterns**

The most common false identity adopted was that of a Caucasian American male (46%), followed by military personnel (12%) - personas carefully chosen to maximize trust and credibility.

7. **Learning Methods**

An overwhelming 80% of fraudsters learned their techniques through peer networks, indicating the existence of informal but effective knowledge-sharing ecosystems among cybercriminals.

CRIMINAL JUSTICE STUDIES
2024, VOL. 37, NO. 4, 328–351
https://doi.org/10.1080/1478601X.2024.2429088

Routledge
Taylor & Francis Group

Examining fifty cases of convicted online romance fraud offenders

Adebayo Benedict Soares [a] and Suleman Lazarus [b,c,d]

[a]Legal and Prosecution Department, Economic and Financial Crimes Commission (EFCC), Abuja, Nigeria; [b]Centre of Excellence on Ageing (CEA), University of Surrey, Guildford, UK; [c]Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), London, UK; [d]Department of Sociology, University of the Western Cape, Cape Town, South Africa

ABSTRACT

This article examines fifty case files of cybercriminals that the Economic and Financial Crimes Commission (EFCC) convicted for online romance fraud. It profiles offenders and explores the value of the Space Transition Theory in understanding digital crimes. Through documentary analysis, the study identifies key patterns in victim demographics, fraudsters' operational strategies, and offenders' socioeconomic backgrounds. Findings reveal a high concentration of U.S. victims (56%) and a preference among offenders for Apple's iPhone (58%). Most offenders presented themselves as Caucasian American males (46%) or military personnel (12%), with some adopting Caucasian European male identities (10%). Victim demographics show a pronounced gender disparity: 70% of offenders primarily targeted female victims, 14% targeted male victims, 10% reached both genders, and 6% did not specify the victims' gender. The analysis also indicates that most offenders were university students (74%), with Facebook (46%) identified as the primary platform for these fraudulent activities. The study emphasizes the need for prevention strategies that genuinely consider the socioeconomic and political conditions that may make online fraud an appealing career option.

ARTICLE HISTORY
Received 9 November 2024
Accepted 10 November 2024

KEYWORDS
Space Transition Theory; online romance fraud; convicted cases; Impersonation of military personnel; Caucasian victims; Scammers prefer Apple; Facebook scams; Yahoo Boys; West African scammers

Introduction

"*Nigerian politician arrested in the United States over $3.3 million romance scam*" (Ugwu, 2024, p.1).

Nigeria has earned a global reputation as a hub for online scams[1] targeting individuals worldwide (Aborisade et al., 2024; Ibrahim, 2016). Conducting research in Nigeria is

CONTACT Suleman Lazarus suleman.lazarus@gmail.com University of Surrey, Stag Hill, Guildford GU2 7XH, UK

This article was originally published with errors, which have now been corrected in the online version. Please see Correction (http://dx.doi.org/10.1080/1478601X.2024.2445400)

[1]The terms "scam" and "fraud," as well as "scammers" and "fraudsters," are used interchangeably throughout this article. While "scam" and "scammers" are widely used in everyday language by the public, media, financial institutions, scambaiters, and government agencies, "fraud" and "fraudsters" are preferred by some academics to reflect the legal and criminological seriousness of these acts. This study adopts both sets of terms to ensure linguistic accessibility for diverse audiences while maintaining the recognition of the serious nature and consequences of these criminal activities.

especially relevant, given its status as a major center for cybercrime. According to the World Cybercrime Index, Nigeria ranks as the leading country in West Africa for cybercrime and is positioned fifth globally (Bruce et al., 2024). These rankings, based on metrics such as technical skill, operational impact, and cashing-out mechanisms, highlight the sophistication of cybercrime in this region.

This notoriety largely arises from the activities of cybercriminals known as 'Yahoo Boys,' who engage in various forms of fraud, including advanced fee fraud (Nigerian 419 scams) (Ibrahim, 2016; Okosun & Ilo, 2023), and, more recently, online romance fraud (Aborisade, Ocheja, & Okuneye, 2024). Over time, these scams have diversified to include cryptocurrency fraud as well (Garba et al., 2024). However, while there has been prior research into the perspectives of scammers (Aransiola & Asindemade, 2011) and their family dynamics (Aborisade, 2022, 2023; Ibrahim, 2017), there are few studies that examine the insights of convicted online fraudsters (Yahoo Boys) in Nigeria (Garba et al., 2024). This study addresses this gap by analysing online romance fraud based on exclusive access to the case files of fifty convicted online romance fraudsters in Nigeria.

Online romance scams typically involve criminals exploiting intimate relationships to gain financial advantage (Bilz et al., 2023; Lazarus et al., 2023), with fraudulent dating profiles serving as the initial point of contact between scammers and potential victims. The primary aim of this research is to investigate these case files to gain a deeper understanding of the profiles of convicted offenders, patterns in victim targeting, and platform use, specifically focusing on romance fraud. This analysis promises to contribute valuable insights into the existing empirical literature, benefiting regional and international stakeholders.

Literature review

Systematic reviews of studies on romance scams, spanning over two decades, consistently underline the deliberate construction of scammer profiles and the nuanced manipulation techniques used to captivate and deceive victims (Bilz et al., 2023; Lazarus et al., 2023). Studies converge on the view that scammers are not merely impersonators but rather highly adaptable manipulators, using flexible narratives tailored to victim responses, amplifying their deceptions' emotional impact (Aborisade et al., 2024; Carter, 2024). Data-driven studies converge on the view that West African scammers are highly adaptable manipulators (e.g., Abubakari, 2024; Aborisade et al., 2024; Lazarus, 2018). They employ flexible narratives tailored to victim responses, thus amplifying the emotional impact of their deceptions. In a qualitative study of 37 offenders, Kopp, Layton, Sillitoe, and Gondal (2015) found that scammers craft profiles with narratives that evolve based on victim responses, enhancing the credibility and impact of their deception. Anesa (2020), focusing similarly on narrative adaptability, observed that scammers use structured message patterns to cultivate emotional dependency, resonating with findings from Kopp et al. This tailored approach is further discussed by Suarez-Tangil et al. (2019) in a quantitative study examining data from over 20,000 offender profiles, noting that scammers often mimic genuine user profiles, complicating detection on dating platforms. Collectively, these studies show that scammers exploit technological and social cues to create credible deceptions, suggesting strategic planning that strengthens their manipulative capabilities.

Similarly, Carter (2024) observed that in romance fraud, rapport-building is crucial, as fraudsters use familiar relationship behaviors to mask their intentions, gain trust and gather personal details that make their personas relatable and credible. With trust secured, they subtly script expectations around loyalty and support, framing future exploitative requests as natural extensions of the relationship (Bilz et al., 2023; Carter, 2024; Lazarus et al., 2023). Collectively, the above scholars demonstrate that fraudsters foster reciprocal trust through crafted storytelling and feigned vulnerability, transforming their manipulation into what feels like a genuine emotional connection.

A recurring theme across studies is the profound psychological and emotional impact of romance scams on victims, extending beyond financial loss (Lazarus et al., 2023). Findings from Whitty and Buchanan (2015), Modic and Anderson (2015), and Cross and Holt (2023) suggest a 'double hit' effect, where the trauma inflicted by scams mirrors the impact of long-term psychological abuse. Whitty and Buchanan (2015), in a qualitative study of 20 victims, and Modic and Anderson (2015), with a large quantitative sample of 6,609 victims, describe a 'double hit' effect, where victims endure compounded trauma from both financial and psychological harm. Cole (2024), through 19 qualitative interviews, further illustrate how these scams can mirror forms of emotional abuse. This consistency in findings underscores the need for support systems to aid both financial and emotional recovery, addressing the mental health toll of romance scams. However, reliance on self-reported data in these studies may introduce potential biases, as individuals might unintentionally reinterpret their trauma. These insights underline the necessity for post-scam support systems that address both financial and emotional recovery, highlighting the mental health impacts of romance scams.

Research reveals significant discrepancies between the fabricated identities of scammers and their actual profiles (Bilz et al., 2023; Carter, 2024; Lazarus et al., 2023). A consistent pattern across studies shows scammers tailoring their demographic claims to high-trust locations like the United States or Europe, capitalizing on perceived credibility. For instance, Edwards et al. (2018) found that scammers often present themselves as nationals from countries with high online dating platform usage, such as the United States (63%), the United Kingdom (11%), and Germany (3%) (Bilz et al., 2023). However, due to the evolving nature of online romance scams, findings from studies like Edwards et al. (2018) should be contextualized within specific timeframes, as these dynamics may change. This temporal consideration is crucial as it reflects scammers' adaptability and how shifts in technology or global events can impact the demographic attributes they use.

Studies also highlight the heightened risks of disclosing personal information in romance scams (Cross & Holt, 2021, 2023). Consistent findings across studies by Cross and Holt (2023), Cross and Lee (2022), and Cross and Holt (2021) show that personal disclosures by victims significantly increase their risk of financial exploitation and physical threats, with scammers exploiting shared information to exert control. Cross and Holt (2023) observed that victims who shared personal information faced increased vulnerability. Cross and Lee (2022) noted that some victims experienced not only financial threats but also feared for their physical safety, including kidnapping threats. Additionally, Cross and Holt (2021) identified scammers' frequent use of fictitious military personas, which tend to resonate with female victims, although gender did not significantly influence economic loss likelihood. These studies suggest that scammers'

manipulation extends beyond financial deceit to emotional and physical threats, broadening the psychological impact on victims.

Although Lazarus et al., (2022) found no gender differences in the perception of socioeconomic cybercrime, including romance scams, Bilz, Shepherd, and Johnson (2023) argue that gender plays a notable role in how scammers construct fraudulent profiles. The misrepresentation of traits like masculinity, financial stability, and cultural identity (Bilz et al., 2023; Edwards et al., 2018; Kopp et al., 2015) suggests a deliberate attempt to align victim expectations with gendered identities strategically tailored to enhance trustworthiness. Kopp et al., (2015) found that male scammer profiles often emphasize traits like masculinity, wealth, humor, and religious devotion, while female profiles project financial independence and occasionally include suggestive elements. Edwards et al. (2018) highlighted frequent misrepresentations of gender, race, and profession, tailored to match the scammer's alleged geographic origin. For example, profiles originating from Malaysia, South Africa, and Nigeria more often present male identities, while those from Senegal, Ukraine, and the Philippines adopt female personas. However, the ease with which scammers alter digital locations using tools like VPNs warrants caution when interpreting geographical indicators in profile analysis. Together, these studies suggest that gendered portrayals are used not merely for deception but to exploit culturally ingrained trust markers, facilitating deeper victim manipulation.

Victim vulnerability is a critical theme in the literature on romance scams, with researchers examining both psychological and socioeconomic factors that may increase susceptibility to fraud (Bilz et al., 2023; Lazarus et al., 2022). Across studies, researchers highlight an interplay between psychological and socioeconomic vulnerabilities, underscoring that susceptibility to scams is rarely due to a single cause (Aborisade et al., 2024; Cole 2024; Snyder & Golladay, 2024). Research on catfishing, a subset of romance scams, identifies specific risk factors associated with victim vulnerability (Snyder & Golladay, 2024). Snyder and Golladay (2024), in a study of 1,511 catfishing victims, found nearly half had been deceived multiple times. Such findings suggest that vulnerability often results from compounding personal and behavioral factors, with repeated victimization reflecting a cycle of manipulation that is difficult to escape. Common tactics include initiating contact, misrepresenting details, avoiding video chats, and requesting financial support, with victims often sending money about half the time. This recurring behavior indicates that while psychological traits make individuals susceptible, scammers' tactics reinforce these vulnerabilities, perpetuating cycles of victimization.

The literature highlights significant limitations in current prevention and detection strategies for romance scams. While Cross and Holt (2021) point to proactive interventions, such as security warnings, Suarez-Tangil et al. (2019) show that sophisticated scammer mimicry complicates detection, especially on platforms lacking advanced textual analysis. Cross and Holt (2021), in a mixed-methods study with 2,478 participants, demonstrate that early interventions like security warnings can reduce susceptibility, suggesting a proactive role for dating platforms in scam prevention. However, the effectiveness of these interventions remains uncertain due to the diversity of platforms and scammer adaptability. Using a large quantitative offender dataset, Suarez-Tangil et al. (2019) propose textual analysis as a technical solution for detecting deceptive profiles. These studies collectively underscore the need for a multi-layered approach combining

technological safeguards and educational efforts, as isolated measures are insufficient against scammers' evolving strategies.

While literature offers substantial insights, there is an underrepresentation of studies exploring scammers' perspectives, with few exceptions (Anesa, 2020; Kopp et al., 2015 using online data sources), which restricts our understanding of offender motivations and psychological profiles. This gap highlights the need for direct examination of convicted offenders, as the absence of their perspectives leaves the understanding of romance scams incomplete. This study addresses this gap by examining case files of convicted online romance scammers prosecuted by the Economic and Financial Crimes Commission (EFCC) in Nigeria.

Economic and financial crimes commission (EFCC)

The Economic and Financial Crimes Commission (EFCC) in Nigeria, established in 2002, was created to tackle various forms of economic crime, especially those committed online, and to restore Nigeria's international reputation (Lazarus & Okolorie, 2019; Pierce, 2016). While the EFCC's establishment marked a significant step toward combating online fraud, the literature emphasizes that Nigeria's reputational issues are multifaceted, with cybercrime being only one contributing factor. Corruption among public officials, highlighted by multiple scholars (Ibrahim, 2016; Ndubueze, 2020; Pierce, 2016), emerges as a persistent theme, indicating that the EFCC's anti-cybercrime efforts alone may be insufficient for reputational repair. Nonetheless, the EFCC is regarded as one of West Africa's most effective agencies in prosecuting cybercrime, as Lazarus and Okolorie (2019) and Orji (2019) noted.

Online offenders in West Africa

The systemic issues facing the Economic and Financial Crimes Commission (EFCC) are mirrored by social factors that influence cybercrime offenders. Research consistently connects cybercrime to socioeconomic pressures and systemic corruption, particularly in countries such as, but not limited to, Ghana (Abubakari & Blaszczyk, 2023) Cameroon (Fuh, 2021), and Nigeria (Lazarus et al., 2022). Qualitative studies highlight that young male offenders, often students, graduates, or school dropouts, are particularly affected (Aransiola & Asindemade, 2011; Ibrahim, 2017; Tade & Aliyu, 2011). This relationship is reinforced through various research methodologies on West African online offenders, including interviews with offenders in Ghana (Abubakari, 2024; Alhassan & Ridwan, 2023), Nigeria (Aransiola & Asindemade, 2011), as well as insights from EFCC officers (Lazarus & Okolorie, 2019). Additionally, research has examined cultural artefacts such as Afrobeats lyrics (Adeduntan, 2022; Lazarus, 2018 Lazarus et al., 2023), and perspectives from high-profile Nigerian cybercriminals convicted in the West (e.g., Lazarus, 2024). Together, these studies highlight the importance of understanding the profiles of offenders.

Cybercrime in Nigeria extends beyond romance scams to related fraudulent activities, such as cryptocurrency scams (e.g., Garba et al., 2024) and business email compromise (e.g., Lazarus, 2024), reinforcing the notion of multi-platform offenders. The overlap between types of online fraud in both empirical (Akanle & Shadare, 2019; Garba et al., 2024; Lazarus, 2024; Aborisade, 2022, 2023) and non-

empirical studies (Hall et al., 2021; Okosun & Ilo, 2023; Ndubueze, 2020) emphasizes the interconnected nature of cybercrime behaviors. This suggests that profiling these offenders requires understanding the spectrum of their activities, as insights into one type of scam often reveal patterns applicable to others, especially motivations. In addition to these insights, our objective is to deepen our understanding of romance scammers and assess the relevance of Space Transition Theory.

Theoretical background

In this study, we examine online romance scams using the lens of Space Transition Theory, as outlined in Table 1. The Space Transition Theory, developed by Jaishankar, provides a framework for examining behavioral changes between physical and virtual spaces (Jaishankar, 2008). This theory suggests that individuals may behave differently when moving from one space to another, often conforming in one setting while engaging in non-conforming actions in another (Jaishankar, 2008). Jaishankar (2008) emphasizes the significance of Space Transition Theory as a guide, in cybercrime research; it is among the few theories specifically designed to explain such behavior. Researchers have increasingly applied this theory to investigate cybercrime in various regions, including Ghana (Danquah & Longe, 2011), and Nigeria (Garba et al., 2024). The Space Transition Theory serves as a valuable framework for understanding how shifts between physical and virtual spaces influence online criminal behavior, offering insights into the dynamics of online romance scams and other digital crimes.

Method and materials

This study employed a documentary analysis method focusing on case files from the Economic and Financial Crimes Commission (EFCC) in Nigeria. A total of fifty cases, all involving convictions for romance scams, were selected from one of the EFCC's Zonal Commands. The sample included convictions secured between 2023

Table 1. Summary of the space transition theory: propositions and key elements.

Proposition Theme	Key Elements	Description
(1) Repressed Criminal Behavior	Physical Space vs. Cyberspace	Offenders may engage in criminal activities in cyberspace that they would not express in the physical world.
(2) Identity Flexibility and Dissociative Anonymity	Cyberspace Characteristics	Anonymity and identity flexibility in cyberspace reduce deterrents, encouraging offenders to engage in cybercrime.
(3) Import-Export of Criminal Behavior	Cyberspace to Physical Space	Criminal behaviors can transfer between physical and digital spaces, highlighting the interconnectedness of these realms.
(4) Intermittent Ventures and Dynamic Nature	Cyberspace Characteristics	The transient nature of cyberspace facilitates evasion of consequences, enabling sporadic criminal activity.
(5) Unification of Strangers and Associates in Cyberspace	Collaboration in Cyberspace	Cyberspace allows for collaboration in criminal activities, either between strangers or associates, across different spaces.
(6) Influence of Closed Societies	Societal Characteristics	Individuals from closed societies may be more likely to engage in cybercrime compared to those from open societies.
(7) Conflict of Norms and Values	Norms Clash	Conflicting norms between physical and cyberspace environments may drive individuals toward cybercrime.

Source: Adapted from Garba, Lazarus, and Button (2024, p. 6).

and 2024, using selection criteria such as the offender's mode of arrest, financial amounts involved, role in the scheme, victim's country, and imposed penalties. This approach provided a structured lens on recent, significant cases within a well-defined timeframe.

Documentary analysis framework

Scott's (2014) framework for document analysis was applied to evaluate the case files based on four criteria: authenticity, credibility, representativeness, and meaning (Platt, 1981). This structured framework enabled a systematic and rigorous review, ensuring the data's validity and relevance to the research questions. Recognizing the potential limitations of documentary sources, often created for non-research purposes, such as prosecution (Denscombe, 2017), the research acknowledged that the case files were initially compiled for legal proceedings, which could introduce contextual limitations (Appleton & Cowley, 1997; Denscombe, 2017).

Recent case files were prioritized to enhance data reliability, aligning with Blackstone's (2019) recommendation to use up-to-date documentation to reduce historical bias. Cross-referencing offenders' handwritten statements with corresponding investigation reports minimized biases and helped verify details across documents. Following methodologies used in similar studies (e.g., Andresen & Button, 2019; Garba et al., 2024), key offender and their victims variables such as age, occupation, gender, and country of origin of victims were documented and investigated. Data were then systematically entered into an Excel spreadsheet to facilitate detailed content analysis and comparative review.

Ethical considerations

Access to sensitive case files required ethical clearance from both law enforcement and academic institutions. The research team included both a law enforcement official and an academic, ensuring a thorough understanding of the cases. The law enforcement officer (A. B. S) secured the official approval number *CB:4000/EFCC/UYO/LEGAL/VOL.1/84* to permit data use, with formal agency approval ensuring compliance with legal requirements for data access. Additionally, to strengthen the ethical rigor, the ethics committee at the second author's (S. L.) university approved the project. All procedures adhered to the standards of the Helsinki Declaration, ensuring participant confidentiality, integrity, and protection.

Data and scope of analysis

This study provides an overview of judicial outcomes ($n = 50$) on a case-by-case basis. Importantly, there were no appeals following any convictions, ensuring that the data represented final legal outcomes. The investigated cases were independent, with no evidence of collaboration among offenders, reflecting individual activities.

Comparative methodology

This methodology aligns with approaches used in prior studies that investigated cybercrime networks through law enforcement data (Lusthaus et al., 2023; Garba et al., 2024; Leukfeldt et al., 2017). Garba et al., (2024) investigated 24 cases in Nigeria, while Leukfeldt et al. (2017) studied eighteen Dutch-based cybercrime cases, both using primary law enforcement data to investigate the characteristics and operations of online fraud. Our study similarly narrows its focus to convicted individuals engaged in romance scams within a defined timeframe and jurisdiction, resulting in a sample size of fifty cases. In parallel, Lusthaus et al. (2023) selected ten UK-based case debriefs based on financial motivations and involvement in major cybercrime activities.

While the methodology offers valuable insights into romance scam offenders, it is limited by the fact that convicted offenders may not represent the broader cybercriminal population. Therefore, these findings should be viewed as a snapshot of romance scam cases within the Nigerian context, contributing empirical data on an understudied area of cybercrime. We present key findings below.

Results

The analysis explores patterns in the demographics of offenders and victims, scammers' learning modes, operational methods, and other unique offender profiles.

Mode of learning romance scam tactics

A significant majority, 80%, as shown in the Figure 1 below, reported learning these tactics through friends, highlighting the role of peer connections in disseminating scam techniques. Meanwhile, 4% learned through online browsing and brothers, indicating that family and independent research play minor roles compared to peer influence. An additional 2% acquired knowledge via a Telegram group and Hustle Academy, a structured cybercrime training environment.

Victims' countries of origin

Among the 50 cases investigated, most victims were from the USA, accounting for 56% (28 cases), followed by victims from unspecified global locations, representing 30% (15 cases), as presented in Table 2. Additional cases involved victims from the Philippines, Brazil, Poland, Canada, and New Zealand, and one joint case from the USA and India, each comprising 2% of the total. The USA's prominence as a source of victims likely reflects the perceived higher wealth and extensive online presence of American users, making them attractive targets for financial exploitation by cybercriminals.

Device brands used by offenders

Scammers exhibited a clear preference for high-end brands, particularly Apple's iPhone, which comprised 58% of the total, followed by Tecno and Samsung devices at 10%, as

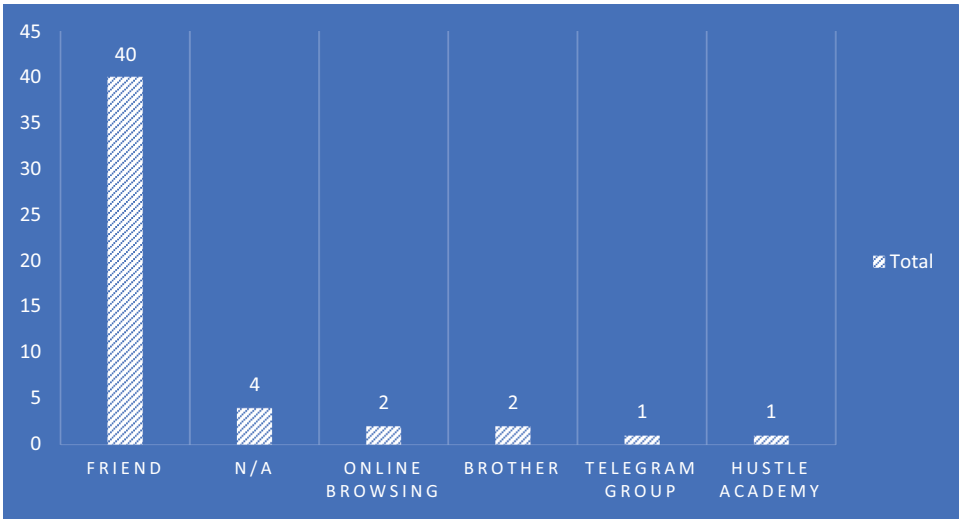

Figure 1. Mode of learning romance scam tactics.

outlined in Table 3 Other brands are detailed in the table below. This pattern indicates that offenders choose devices to boost their credibility, likely utilizing reputable brands like Apple's reliability and symbol status.

Cover Stories and Identities Adopted by Scammers

The identities scammers employed were predominantly Caucasian American males (23 cases), as shown in Table 4. This choice was likely influenced by the perceived

Table 2. Detailed victims' countries of origin with percentages.

Country of Origin	Number of Cases	Percentage (%)
USA	28	56
Global	15	30
Brazil	1	2
Poland	1	2
Canada	1	2
New Zealand	1	2
USA & India	1	2
N/A	1	2

Table 3. Device brands used by offenders with percentages.

Device Brand	Number of Offenders	Percentage (%)
iPhone	29	58
Tecno	5	10
Samsung	5	10
Redmi	3	6
HP	3	6
Huawei	2	4
Infinix	1	2

Table 4. Cover stories and identities used by offenders.

Cover Story Identity	Number of Cases	Percentage (%)
Caucasian American Male	23	46
Military Officer	6	12
Female	6	12
Caucasian Male	3	6
Male/Female Combo	3	6
British Male	1	2
Jamaican Male	1	2
Caucasian European Male	1	2
Engineer	1	2
Indian Male	1	2
American Doctor	1	2
Multiple Identities	1	2

trustworthiness and social familiarity associated with this demographic among victims. Military and female identities were also common, each used in six cases. Adopting identities such as military personnel, engineers, and doctors appears to be a strategic choice to foster rapport and convey stability, enhancing scammers' success in deceiving victims.

Occupational background of offenders

A significant percentage of perpetrators (74%) were undergraduate students, followed by graduates at 16%, as shown in Figure 2 below. The prevalence of university students among offenders points to economic instability and limited legitimate employment opportunities, driving these individuals toward cybercrime.

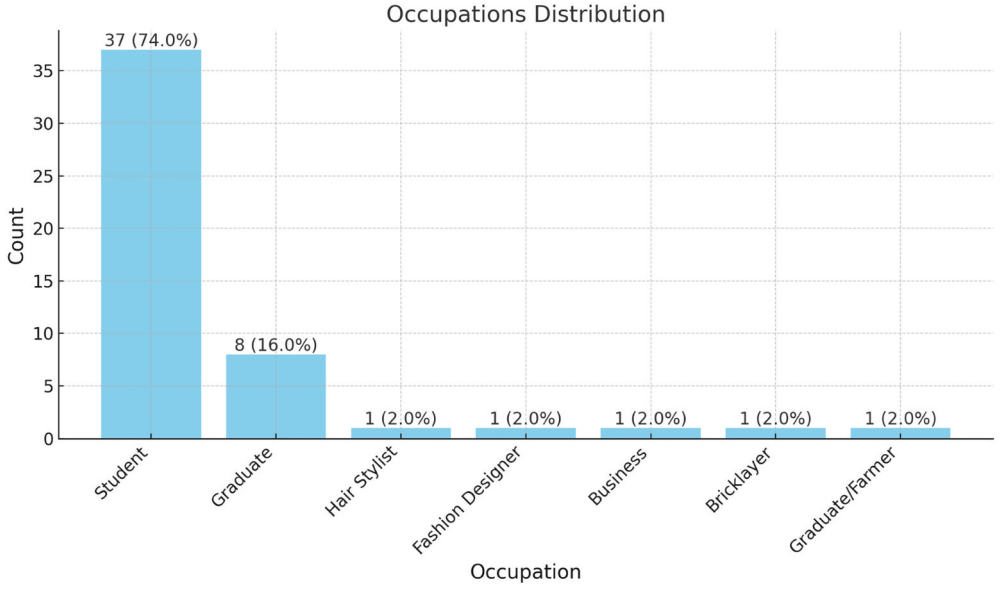

Figure 2. Occupations of offenders.

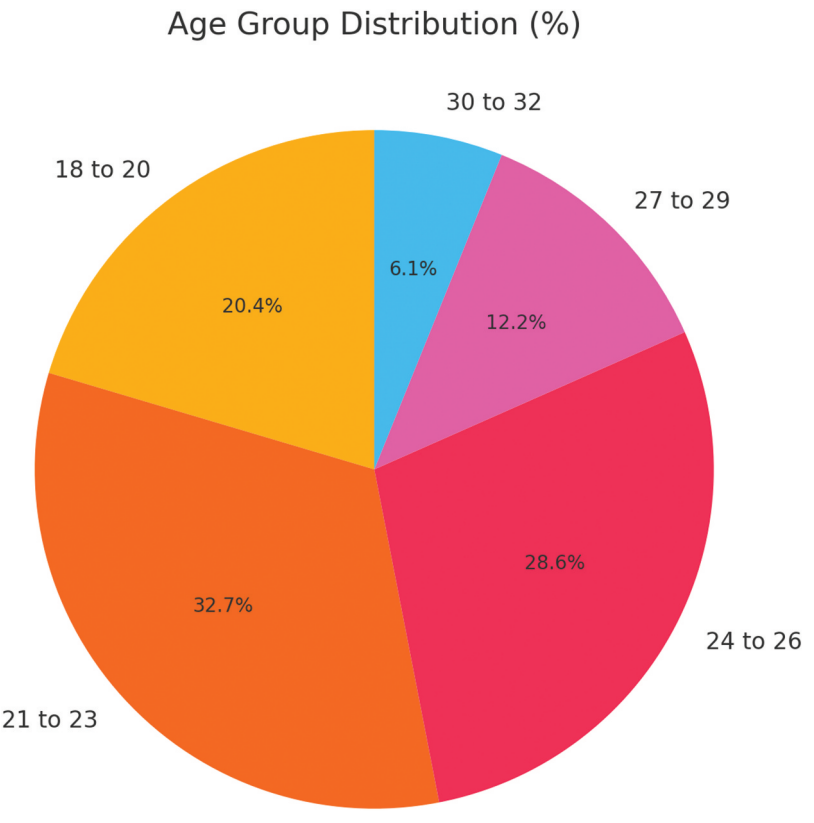

Figure 3. Age of the offenders.

Age distribution of offenders

Offenders' ages predominantly ranged from 18 to 32, with the majority being between 18 and 26, collectively accounting for 81.7% of offenders as illustrated in the Figure 3 below. This age range aligns with younger demographics' familiarity with digital platforms, facilitating engagement in online scams. The intersection between youth, economic pressures, and involvement in cybercrime highlights a demographic segment particularly susceptible to engaging in romance scams.

Platforms used by scammers

Scammers leveraged several social media platforms, with Facebook used in 46% of cases (23 offenders), followed by Facebook & Instagram (8 cases), Instagram alone (5 cases), and others listed in Table 5. Facebook's extensive user base and interpersonal features likely contribute to its popularity among scammers, while Instagram offers tools for creating convincing online personas.

Table 5. Platforms used by scammers with percentages.

Platform	Number of Cases	Percentage (%)
Facebook	23	46
Facebook & Instagram	8	16
Instagram	5	10
WhatsApp & Instagram	4	8
Email	5	10
TikTok	2	4
Twitter (X)	1	2
Skype	1	2
Telegram	1	2

Motivational factors behind offenders' involvement

Financial need emerged as the primary motivator among all offenders (n=50). This finding aligns with broader empirical literature on West Africa, which highlights how economic desperation or the appeal of financial gain drives individuals toward cybercriminal activities. This finding highlights the socioeconomic factors at play in young Nigerians' involvement in romance scams.

Victim loss and fake profiles

Offenders collectively created 128 fake profiles and emails to facilitate their scams, resulting in a cumulative financial loss of $31,488 among victims. This reflects a high degree of strategic planning, as offenders maintained multiple fake identities to expand their reach and evade detection.

Gender of victims

The analysis of victim demographics across fifty convicted cases of online romance scammers reveals a pronounced gender disparity. Among the cases, 35 offenders (70%) primarily targeted female victims, indicating a significant gendered pattern in victim selection. In contrast, seven scammers (14%) focused on male victims, while five (10%) targeted both genders. Additionally, three scammers (6%) did not specify the gender of their victims, suggesting either a lack of transparency or a deliberate choice in record-keeping. This distribution implies that female victims are disproportionately targeted in romance scams.

Discussion

Gender, occupation, and demographics of offenders

An analysis of fifty convicted cases of online romance scammers provides a demographic profile of cybercrime offenders in Nigeria, revealing a significant gender pattern: all convicted individuals were male, representing a 100% male prosecution rate by the EFCC for romance scams. This predominance aligns with the broader literature on Nigerian cybercrime, where a male-dominated culture emerges from socioeconomic pressures and is reinforced by traditional gender

norms[2]. Although the dominant discourse on online romance fraud in West Africa focuses on male perpetrators (e.g., Lazarus, Whittaker, McGuire & Platt, 2023), Abubakari (2023) offers a contrasting perspective by examining female participation. Nevertheless, Abubakari's (2023) findings concur with existing research on male perspectives by identifying economic pressures as a shared motivating factor. This alignment is evident in studies such as those by Aransiola and Asindemade (2011), which focused exclusively on male cybercriminals, and in Lazarus et al. (2023), who analyzed lyrics from artists who were predominantly male (97%).

Studies by Kopp et al., (2015) and Anesa (2020) are reflective of these findings, noting that male offenders often employ sophisticated profile construction techniques to exploit relational vulnerabilities in female victims. Research by Garba et al., (2024) further corroborates this pattern, showing that young Nigerian men, primarily aged[3] 18 to 34, are disproportionately involved in cybercrime. Similarly, Alhassan and Ridwan (2023) highlight that Ghanaian males, primarily aged 17 to 25, are also heavily represented in such activities. The findings also resonate with the arguments of Lazarus and Okolorie (2019), who suggest that Nigerian men may turn to online fraud as a way to assert masculinity and fulfill societal expectations in the absence of legitimate economic opportunities. Lazarus's et al., (2022, pp. 1–8) research argues that economic hardship plays a significant role in this trend, with young men seeing cybercrime as a viable alternative in a context where political figures, often termed 'Yahoo men,' engage in widespread embezzlement. Similarly, Ugwu (2024) reported that a Nigerian politician was arrested in the United States for a $3.3 million romance scam. Therefore, we contend that this parallel effectively blurs the distinction between 'Yahoo Boys' (online scammers) and corrupt politicians ('Yahoo men'), embedding cybercrime within a broader socio-political context and complicating efforts to discourage youths from such criminal schemes.

Educational background is also notable, with university students (74%) significantly represented among offenders. Studies by Akanle and Shadare (2019), Aransiola and Asindemade (2011), and Tade and Aliyu (2011) identify university students as a demographic subgroup frequently involved in cybercriminal activities. Higher education, coupled with limited legitimate job prospects, appears to facilitate entry into online fraud. This link between education and cybercrime underscores the role of socioeconomic aspirations, where higher education serves as both an asset and a constraint when conventional job opportunities are lacking. The convergence between this study's findings and previous research highlights the socioeconomic and gendered dimensions of cybercriminal activities in Nigeria, providing insight into the motivations driving young Nigerian men toward online romance scams.

Regional distribution: North-South divide

Another key finding is the distinct North-South divide among offenders, with all convicted scammers originating from southern Nigeria. This aspect of our findings aligns with the literature, which asserts that crime is inherently spatial, influencing behavior both within

[2] Economic hardship alone does not directly cause crime, but it can be a contributing factor.
[3] These cybercriminals (Yahoo Boys) are aged 18 to 34, with individuals under 30 comprising at least 75% of the population.

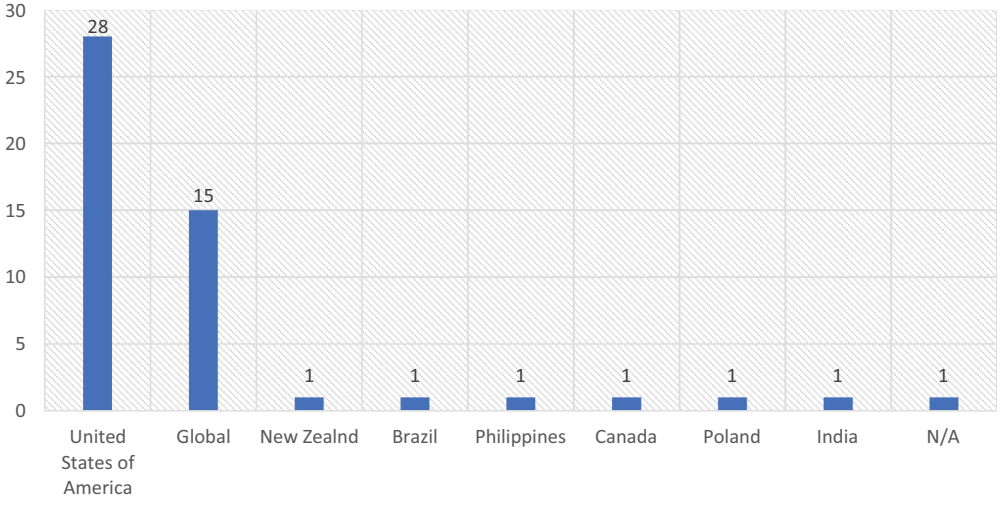

Figure 4. Countries of online romance fraud victims.

and across locations (Hall & Yarwood, 2024; Hall et al., 2021; Lazarus & Button, 2022a). This geographical concentration is revealing. Specifically, scholars argue that the enduring disparities in the production of cybercrime in Nigeria are rooted in the legacy of British colonialism, particularly the merging of the northern and southern regions despite their distinct differences (Lazarus & Button, 2022a, 2022b).

"*Colonialism is the base that shaped the superstructure comprising political, religious, historical, geological (e.g., crude oil), and economic factors...regional differences in educational attainment, originating from differing experiences of Christianization and colonization, interact with regional disparities in the production of cybercrime*" (Lazarus & Button, 2022a, p. 504).

Although Lazarus and Button (2022a) documented a regional skew in cybercrime, our findings warrant careful interpretation. The southern location of the EFCC's zonal office, from which the case files were sourced, may influence this pattern. Additionally, the sample size of fifty cases may limit the generalizability of this regional finding. Nevertheless, the North-South divide in cybercrime production and prosecution remains crucial for further research to better understand regional dynamics in cybercriminal activities.

Countries of romance fraud victims

Our results indicate that most victims targeted by these scammers are from the United States (56%), followed by a smaller percentage from unspecified global locations (30%) and other countries, as shown in the Figure 4 below. The dominance of U.S. victims aligns with previous studies, such as Garba et al., (2024) on cryptocurrency fraudsters.

The prominence of U.S. victims supports the notion that cybercriminals target individuals perceived to have higher financial resources and a strong online presence, as noted in media sources (e.g., Essien, 2022), and scholarly findings (e.g.,

Garba et al., 2024). This targeting pattern aligns with Whitty and Buchanan (2015) and Modic and Anderson (2015), who argue that scammers prioritize victims seen as financially secure, often through elaborate grooming processes. This finding challenges claims by Akanle et al., (2016) and Bello and Griffiths (2021) that Nigeria's cybercrime prevalence is primarily due to weak law enforcement, instead suggesting that Nigerian agencies, such as the EFCC, employ intelligence-led methods to target and prosecute cybercriminals effectively.

The gender of victims also displayed a pronounced disparity, with 70% of offenders targeting female victims, 14% targeting male victims, and 10% targeting both genders. This aspect of our findings reflects Whitty's (2019) findings in the United Kingdom, which document similar gender disparities in romance fraud victimization. This also aligns with Sorrell and Whitty (2019), who suggest that female victims, particularly those with specific personality traits, may be more susceptible to online scams due to trust dynamics in romantic contexts. The predominance of female victims suggests a need for awareness campaigns tailored to this demographic on dating platforms.

Parasitic platform criminality

Facebook was the most frequently used platform, appearing in 46% of cases, followed by Instagram and WhatsApp. Its large user base and social networking features make it appealing to scammers seeking to forge connections and create convincing personas. This observation aligns with findings by Cross and Holt (2021) and Lazarus (2024), who describe how popular platforms facilitate scammer-victim interactions by enabling profile manipulation. The Space Transition Theory, emphasizing the fluidity of cyberspace, applies here as offenders exploit the ease of creating and discarding fake profiles to evade detection. Lazarus (2024) explains this phenomenon as 'parasitic platform criminality,' where 'cybercriminals turn legal apps offered by platform providers into a discordant symphony of malice to advance their unlawful pursuits' (p.15). This innovation threatens the reputation and integrity of industry giants like Facebook, Apple, Google, and Yahoo, exposing their vulnerabilities to scams and platform misuse.

Financial motivations and implications

Financial need has emerged as the primary motivator for all offenders, underscoring the economic factors driving cybercrime engagement as offenders. While the lens of Space Transition Theory primarily focuses on the structural and behavioural dynamics of cyberspace, it does not directly address financial incentives and motivations. However, its 'intermittent ventures' concept provides a framework for understanding how offenders exploit cyberspace's dynamic nature to maximize financial gains. Nearly all cybercrime offenses in Nigeria primarily stem from economic motivations, according to Ibrahim's (2016) Tripartite Cybercrime Framework.[4] The framework complements the Space

[4]The motivational framework by Ibrahim (2016) posits that cybercrime can be motivated by socioeconomic, psychosocial, and geopolitical factors. While cybercrime in other nations, particularly Western countries, may involve all three, in Nigeria, it is fundamentally rooted in socioeconomic factors (see Ibrahim 2016 for detailed analysis).

Transition Theory by explicitly offering insights into the socioeconomic drivers of cybercrime, particularly within Nigeria.

Research on socioeconomic motivations, including empirical studies by Ogundele et al. (2023), Akanle and Shadare (2019), Garba et al., (2024) and Lazarus and Okolorie (2019), aligns with this study's finding that many scammers are driven by socioeconomic needs, with 74% identified as university students. Further insights from Sorell and Whitty's (2019) study on scam victims suggest that, although victims may sometimes share a degree of responsibility for their financial losses, the consequences they face are often disproportionately severe relative to any imprudence on their part. This highlights the complexity of assigning responsibility, particularly given the manipulation tactics scammers use. For example, Wang and Zhou (2022) demonstrate how scammers cultivate emotional attachment through fabricated personal details and shared interests, prompting victims to suspend rational judgment. Similarly, Whitty and Buchanan (2015) emphasize the coercive techniques that position victims as targets rather than contributors to their own victimization. These differing perspectives highlight the need for nuanced research that acknowledges the agency of scammers without shifting undue responsibility onto victims, especially given the manipulative and coercive nature of romance scams.

Theoretical implications: The Space Transition Theory

The Space Transition Theory posits that individuals may exhibit behaviors in cyberspace that differ significantly from those in physical spaces, due to the anonymity and dissociative characteristics offered by the digital realm (Jaishankar, 2008). The findings of this study align with the Space Transition Theory's concepts, particularly regarding the flexibility of identity and the dissociative anonymity in cyberspace, which offenders exploit to enhance their credibility and manipulate victims. A notable example is the frequent adoption of identities like Caucasian American males (46%) and military personnel (12%), which are strategically crafted to build trust with victims by conforming to stereotypically trustworthy profiles.

This pattern also echoes findings by Cross and Holt (2021), and Abubakari (2024), who observed that scammers often use fictitious military personas, especially in targeting female victims. Our study corroborates this, showing a pronounced gender disparity among victims, with 70% of offenders primarily targeting women and only 14% targeting men. Although Cross and Holt (2021) found that gender did not necessarily influence the likelihood of financial loss, this choice of identity likely taps into relational vulnerabilities that are often more pronounced in female victims (Whitty, 2019). This highlights a paradox: digital spaces, including dating platforms, provide women with new freedoms and opportunities for empowerment (Morahan-Martin, 2000; Young & Roberts, 2021). At the same time, they expose women to online hostility, heighten risks of exploitation, and reinforce gender inequalities in the digital age (Morahan-Martin, 2000; Gillett, 2021; Steinmetz et al., 2019; Lazarus et al., 2022). Thus, the Space Transition Theory's notion of dissociative anonymity is vividly illustrated in these impersonations, which allow scammers to transcend the limitations of their actual identities and assume roles perceived as socially credible and trustworthy.

Beyond that, these findings mirror Abubakari (2024) and, Suarez-Tangil et al. (2019), who highlighted the prevalence of fake profiles designed to appear authentic and relatable. This strategic use of fabricated personas aligns with the Space Transition Theory's assertion that cyberspace fosters behaviors that may not occur in physical spaces due to social and legal constraints. In the digital environment, offenders capitalize on the fluidity of identity, constructing personas that would be implausible or impossible to maintain in real life, thereby enabling manipulation on a scale and depth unique to the cyber domain.

However, the Nigerian context presents a unique challenge to the broad application within the framework of Space Transition Theory, as this study's findings indicate that local socioeconomic pressures are crucial drivers of cybercriminal behavior, rather than cyberspace anonymity alone. While the lens of Space Transition Theory (outlined in Table 1) suggests that individuals may engage in criminal activities online that they would not pursue in physical spaces (Proposition 1: Repressed Criminal Behavior), our results reveal that Nigerian men are disproportionately involved in online romance scams. These crimes are driven more by socioeconomic factors than by the virtual affordances of anonymity and dissociative identity. In Nigeria, online criminal tendencies arise from economic necessity, not purely digital disinhibition.

However, some might argue that these trends reflect regional dynamics rather than inherent weaknesses in the Space Transition Theory. Therefore, a cybercrime theory conceptualized in 2008 may face challenges in fully addressing the complexities of digital crimes 16 years later, given the rapid evolution of technology and criminal methodologies. This spotlights the importance of contextual and cultural sensitivity and highlights the need for theoretical updates to address the evolving dynamics of cybercrime.

Our findings also reveal that offenders exploit identity flexibility and dissociative anonymity (Proposition 2) to create convincing personas that facilitate trust and deception. This study shows that Nigerian online romance fraudsters adopt identities such as Caucasian American males (46%) or military personnel (12%), profiles that resonate with gendered expectations and relational vulnerabilities, particularly among female victims. This aligns closely with the Space Transition Theory's notion that cyberspace anonymity reduces deterrents; however, our data suggest that impersonations in romance scams are crafted to meet socio-cultural expectations in target countries, indicating a complex interplay between digital affordances and social motivations.

Moreover, the Space Transition Theory's concept of the import-export of criminal behavior (Proposition 3), where criminal tendencies transfer between physical and cyberspace, is evident in Nigeria. Economic drivers like unemployment and financial pressures in the physical world find an outlet in the virtual realm, with offenders using cyberspace as a means to achieve financial success unattainable through legitimate means in their immediate environment. Thus, cybercrime here extends from socioeconomic conditions in the physical space rather than a behavior shift solely due to online anonymity.

Furthermore, the transient nature of cyberspace (Proposition 4) allows offenders to engage in romance scams sporadically, adapting and abandoning profiles as needed to evade detection. Combined with Nigeria's socioeconomic constraints, this dynamic feature enables offenders to continue their schemes with relative anonymity. However,

this intermittency arises not only from cyberspace's fluidity but also from the need to balance risk and gain, with offenders cycling through scams to cope with economic instability.

Space Transition Theory's focus on closed societies (Proposition 6) offers insight into the drivers of cybercrime in Nigeria. Given that many Nigerians experience severe poverty and live in conditions of abject deprivation, Nigerian society often restricts legitimate paths to economic stability. Consequently, this restriction increases the appeal of cybercrime as an alternative means of livelihood. The pressure to achieve financial success within a culturally closed environment pushes young men to seek wealth through digital means. Here, the Space Transition Theory's closed-society influence resonates with the Nigerian context. Still, our findings underline that this influence is closely intertwined with structural socioeconomic constraints distinct from the theory's generalized application. Thus, while the lens of Space Transition Theory provides a foundation for understanding some aspects of romance scams, this study reveals that cybercriminal behavior among Nigerian offenders is not merely a result of digital affordances. Instead, it is deeply rooted in local socioeconomic pressures, cultural norms, and gendered expectations that shape and intensify motivations to engage in cybercrime. This indicates that the Nigerian context requires a nuanced application of the Space Transition Theory, integrating the digital dynamics of cyberspace with the socioeconomic realities of the physical world.

Limitations and future research directions

While this study offers valuable insights into the profiles and operational methods of convicted romance scammers in Nigeria, it is limited by its sample size and geographic scope. The reliance on case files from one of the EFCC's Zonal Commands in southern Nigeria may influence regional findings, and the sample of fifty cases may not capture the full diversity of cybercriminal behavior in the country. Future research should expand the sample size and include data from multiple EFCC Zonal Commands across Nigeria for a more comprehensive understanding of cybercrime trends. Additionally, further studies could investigate the role of social media platforms in enabling romance fraud.

Conclusion

This study examines fifty case files of convicted online romance scammers prosecuted by the Economic and Financial Crimes Commission (EFCC). Through an analysis of offenders' profiles, victim demographics, and operational strategies, this research offers valuable insights into the characteristics and motivations of cybercriminals involved in romance scams. Key findings highlight the predominance of male offenders, primarily young university students. These offenders are influenced by socioeconomic pressures and gendered expectations deeply rooted in Nigerian society. Figures 2 and 3 illustrate these dynamics, shedding light on the intersection of economic hardship and societal norms and expectations that shape their involvement in cybercrime. The analysis also underscores the strategic use of digital platforms, with Facebook emerging as the primary platform for establishing trust and manipulating victims, most of whom were U.S.-based and predominantly female.

Table 6. Summary of research focus, key findings, and theoretical framework.

Category	Details
Research Focus	Analysis of fifty case files of convicted online romance scammers in Nigeria, prosecuted by the Economic and Financial Crimes Commission (EFCC)
Key Findings	- Predominantly male offenders (100%), mostly young university students - Major target demographic: U.S. victims (56%), primarily female (70%) - High-end devices favored by offenders, with iPhones as the most common - Offenders frequently portrayed Caucasian American males (46%) and military personnel (12%) - Facebook identified as the primary platform used for initiating scams - 80% learned romance scam tactics through friends
Theoretical Framework	The Space Transition Theory
Theoretical Insights	- Cyberspace anonymity and identity flexibility facilitate online romance scams - While the Space Transition Theory remains a foundational framework, its 2008 conceptualization may not fully address the complexities of present-day digital crimes, given the evolving realities of cybercrime
Regional Findings	- All offenders originated from southern Nigeria - Possible sampling bias due to case files sourced from a single EFCC office in southern Nigeria
Policy Implications	- Strengthen law enforcement strategies to combat online romance scams - Develop public awareness campaigns targeting high-risk victim demographics (e.g., U.S. females) - Address socioeconomic drivers of cybercrime through employment and education initiatives
Limitations	- Limited to fifty cases from one EFCC office, potentially influencing regional findings - Further research needed on female offenders and the gendered nature of victimization
Recommendations for Future Research	- Broaden sample size and include multiple regions within Nigeria for a more comprehensive understanding - Explore gender dynamics in cybercrime, including female perpetrators and victims - Examine how different digital platforms contribute to varying methods in cybercrime

Using the Space Transition Theory as a guide, this study emphasizes how the anonymity and identity flexibility of cyberspace facilitate criminal activities. These features enable offenders to exploit victims' relational vulnerabilities through fabricated personas. However, the findings challenge some assumptions within the theory, suggesting that in Nigeria, socioeconomic and cultural factors exert a stronger influence on cybercriminal behavior than cyberspace anonymity alone. This highlights the need for theoretical frameworks incorporating local socioeconomic conditions and cultural norms to explain cybercrime.

To provide a consolidated overview of this study's contributions, Table 6 below summarizes key findings, theoretical insights, limitations, and recommendations for future research. This summary encapsulates our work's practical and theoretical implications of our work. It offers a foundation for further investigation into the socioeconomic drivers of cybercrime and the efficacy of targeted intervention strategies.

This study stresses the need for a multi-faceted approach to combating online romance scams, focusing not only on strengthening law enforcement but also on addressing the socioeconomic issues that drive individuals toward cybercrime. Targeted policy interventions, public awareness campaigns, and improved digital literacy are critical in mitigating cybercrime's impact. As digital connectivity grows both within Nigeria and globally, understanding the socioeconomic, cultural, and digital behaviors that shape cybercriminal activity will be essential for developing effective prevention strategies. This study thus lays the groundwork for future research and efforts to address the complex interplay of factors sustaining online romance scams and other forms of socioeconomic cybercrime.

Acknowledgments

We are grateful to our Creator for blessing this collaboration between academia and law enforcement. Dr. Suleman Lazarus presented part of this research at the UK Government Counter Fraud Profession's 2024 annual conference in Birmingham. We also extend our sincere thanks to the editors and reviewers for their invaluable feedback, which has enriched this work.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

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

Notes on contributors

Adebayo Benedict Soares is a superintendent and senior prosecutor at Nigeria's Economic and Financial Crimes Commission (EFCC). He is a Certified Economic Crime Forensic Examiner (CECFE), Certified Cybercrime Investigator (CCCI), and Certified Fraud Examiner (CFE). He holds a Master of Science in Economic Crime and International Criminal Justice, as well as an Executive Diploma in Anti-Corruption and Diplomacy. Mr. Soares brings extensive expertise in investigating and prosecuting economic crimes. Mr. Soares has successfully investigated and prosecuted numerous financial crimes, including those involving international law enforcement agencies. He has secured convictions in cases of investment fraud, advance fee fraud, forgery, bank fraud, money laundering, corruption, and cybercrime and has been instrumental in asset recovery through civil forfeiture. Mr. Soares also regularly provides training and presentations on fraud, AML/CFT guidelines, corruption, and cybercrime to banks, government institutions, and youth groups.

Suleman Lazarus holds a PhD from the University of Portsmouth and is an Associate Editor for the Association for Computing Machinery (ACM) journal "Digital Threats: Research and Practice." Dr Lazarus serves as a Visiting Fellow at the Mannheim Centre for Criminology at the London School of Economics and Political Science (LSE) and is a Fellow at the Department of Sociology, University of the Western Cape, South Africa and the University of Surrey, UK. He created the "Tripartite Cybercrime Framework (TCF)," categorising cybercrimes into socioeconomic, psychosocial, and geopolitical motivational groups. His scholarly works, primarily focusing on cybercriminals and society, have been featured in journals like "Telematics and Informatics," "Deviant Behavior," "Cyberpsychology, Behavior and Social Networking," and "Current Issues in Criminal Justice."

ORCID

Adebayo Benedict Soares http://orcid.org/0009-0000-4303-9368
Suleman Lazarus http://orcid.org/0000-0003-1721-8519

Data availability statement

Access to datasets may be granted upon reasonable request and with appropriate permissions, in compliance with confidentiality agreements.

Permission to reproduce material

Permission to reproduce material from other sources was not required.

Ethics approval statement

The primary Ethics approval for this study was obtained from the following institution: Economic and Financial Crimes Commission (EFCC), Nigeria (CB:4000/EFCC/UYO/LEGAL/VOL.1/84)

References

Aborisade, R. A. (2022). Internet scamming and the techniques of neutralization: Parents' excuses and justifications for children's involvement in online dating fraud in Nigeria. *International Annals of Criminology*, *60*(2), 199–219. https://doi.org/10.1017/cri.2022.13

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

Abubakari, Y. (2023). The espouse of women in the online romance fraud world: Role of sociocultural experiences and digital technologies. *Deviant Behavior*, *45*(5), 708–735. https://doi.org/10.1080/01639625.2023.2263137

Abubakari, Y. (2024). Modelling the modus operandi of online romance fraud: Perspectives of online romance fraudsters. *Journal of Economic Criminology*, *100112*, 1–13. https://doi.org/10.1016/j.jeconc.2024.100112

Abubakari, Y., & Blaszczyk, M. (2023). Politicization of economic cybercrime: Perceptions among Ghanaian Facebook users. *Deviant Behavior*, *45*(4), 483–502. https://doi.org/10.1080/01639625.2023.2253487

Adeduntan, A. (2022). Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. Journal of Popular Music. *Journal of Popular Music Studies* , *34*(1), 44–67. https://doi.org/10.1525/jpms.2022.34.1.44

Akanle, O., Adesina, J. O., & Akarah, E. P. (2016). Towards human dignity and the internet: The cybercrime (*yahoo yahoo*) phenomenon in Nigeria. *African Journal of Science, Technology, Innovation & Development*, *8*(2), 213–220. https://doi.org/10.1080/20421338.2016.1147209

Akanle, O., & Shadare, B. R. (2019). Yahoo-Plus in Ibadan: Meaning, characterization and strategies. *International Journal of Cyber Criminology*, *13*(2), 343–357.

Alhassan, A. R. K., & Ridwan, A. (2023). Identity expression—the case of 'Sakawa' boys in Ghana. *Human Arenas*, *6*(2), 242–263. https://doi.org/10.1007/s42087-021-00227-w

Andresen, M. S., & Button, M. (2019). The profile and detection of bribery in Norway and England & Wales: A comparative study. *European Journal of Criminology*, *16*(1), 18–40. https://doi.org/10.1177/1477370818764827

Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, *35*(100398), 1–8. https://doi.org/10.1016/j.dcm.2020.100398

Appleton, J. V., & Cowley, S. (1997). Analysing clinical practice guidelines. A method of documentary analysis. *Journal of Advanced Nursing*, *25*(5), 1008–1017. https://doi.org/10.1046/j.1365-2648.1997.19970251008.x

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

Bello, M., & Griffiths, M. (2021). Routine activity theory and cybercrime investigation in Nigeria: How capable are law enforcement agencies? In T. Owen & J. Marshall (Eds.), *Rethinking cybercrime* (pp. 213–228). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-55841-3_11

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers*, *35*(6), 773–788. https://doi.org/10.1093/iwc/iwad048

Blackstone, A. (2019). *Social research: Qualitative and quantitative methods*. FlatWorld.

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., Varese, F., & Jan, N. (2024). Mapping the global geography of cybercrime with the world cybercrime index. *PLoS One*, *19*(4), e0297312. https://doi.org/10.1371/journal.pone.0297312

Carter, E. (2024). *The language of romance crimes: Interactions of love, money, and threat*. Cambridge University Press.

Cole, R. (2024). A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States. *Journal of Economic Criminology*, *100108*, 1–14. https://doi.org/10.1016/j.jeconc.2024.100108

Cross, C., & Holt, T. J. (2021). The use of military profiles in romance fraud schemes. *Victims & Offenders*, *16*(3), 385–406. https://doi.org/10.1080/15564886.2020.1850582

Cross, C., & Holt, T. J. (2023). More than money: Examining the potential exposure of romance fraud victims to identity crime. *Global Crime*, *24*(2), 107–121. https://doi.org/10.1080/17440572.2023.2185607

Cross, C., & Lee, M. (2022). Exploring fear of crime for those targeted by romance fraud. *Victims & Offenders*, *17*(5), 735–755. https://doi.org/10.1080/15564886.2021.2018080

Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: The case of Ghana and beyond. *African Journal of Computing & ICT*, *4*(2), 37–48.

Denscombe, M. (2017). *The good research guide: For small-scale social research projects*. McGraw-Hill Education.

Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2018). The geography of online dating fraud. In *Workshop on Technology and Consumer Protection (ConPro)*, San Francisco, California (pp. 1–7).

Essien, H. (2022). *Over half of Nigerians in our prisons jailed for fraud: THE UNITED STATES govt*. Peoples gazette. https://gazettengr.com/over-half-of-nigerians-in-our-prisons-jailed-for-fraud-u-s-govt/

Fuh, D. (2021). Chihuahua promises and the notorious economy of fake pets in Cameroon. *Journal of African Cultural Studies*, *33*(3), 387–403. https://doi.org/10.1080/13696815.2021.1949967

Garba, K. H., Lazarus, S., & Button, M. (2024). An assessment of convicted cryptocurrency fraudsters. *Current Issues in Criminal Justice*, *37*, 1–17. https://doi.org/10.1080/10345329.2024.2403294

Gillett, R. (2021). "This is not a nice safe space": Investigating women's safety work on Tinder. *Feminist Media Studies*, *23*(1), 199–215. https://doi.org/10.1080/14680777.2021.1948884

Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). *Economic geographies of the illegal: the multiscalar production of cybercrime* (Vol. 24, pp. 282–307). https://doi.org/10.1007/s12117-020-09392-w

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

Ibrahim, S. (2016). 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. (2017, June 12–14). Causes of socioeconomic cybercrime in Nigeria. *Paper presented at the IEEE International Conference on Cybercrime and Computer Forensics (ICCCF)*, (pp. 1–9). Vancouver, BC, Canada. https://doi.org/10.1109/ICCCF.2016.7740439

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the internet* (pp. 283–301). Prentice Hall.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, *9*(2), 205.

Lazarus, S. (2018). Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip Hop Artists, *Criminology, Criminal Justice, Law & Society*, *19*(2), 63–80.
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. (2022a). 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., & Button, M. (2022b). Online fraudsters, colonial legacies, and the north-south divide in Nigeria. *The Conversation*. Retrieved from https://theconversation.com/online-fraudsters-colonial-legacies-and-the-north-south-divide-in-nigeria-187879
Lazarus, S., Button, M., & Adogame, A. (2022). Advantageous comparison: Using twitter responses to understand similarities between cybercriminals ("yahoo boys") and politicians ("yahoo men"). *Heliyon Elsevier*, *8*(11), e11142. https://doi.org/10.1016/j.heliyon.2022.e11142
Lazarus, S., Button, M., & Kapend, R. (2022). 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., & 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., 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), 1–17. https://doi.org/10.1016/j.jeconc.2023.100033
Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 – 2021). *Journal of Economic Criminology*, *2*, 100013. https://doi.org/10.1016/j.jeconc.2023.100013
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, *67*, 21–37. https://doi.org/10.1007/s10611-016-9662-2
Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, *27*, 1–24. https://doi.org/10.1007/s12117-022-09476-9
Modic, D., & Anderson, R. (2015). It's all over but the crying: The emotional and financial impact of internet fraud. *IEEE Security & Privacy*, *13*(5), 99–103. https://doi.org/10.1109/MSP.2015.107
Morahan-Martin, J. (2000). Women and the internet: Promise and perils. *Cyberpsychology & Behavior*, *3*(5), 683–691. https://doi.org/10.1089/10949310050191683
Ndubueze, P. N. (2020). Cybercrime and legislation in an African context. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and Cyberdeviance* (pp. 345–364). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_74
Ogundele A. T., Awodiran M. A., Idem U. J., & Anwana E. O. (2023). Cybercrime activities and the emergence of yahoo boys in Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, Bangkok, Thailand (pp. 313–320). IEEE. https://doi.org/10.1109/CyMaEn57228.2023.10051083
Okosun, O., & Ilo, U. (2023). The evolution of the Nigerian prince scam. *Journal of Financial Crime*, *30*(6), 1653–1663. https://doi.org/10.1108/JFC-08-2022-0185
Orji, U. J. (2019). An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. *Computer Law & Security Review*, *35*(6), 105330. https://doi.org/10.1016/j.clsr.2019.06.001
Pierce, S. (2016). *Moral economies of corruption*. Duke University Press.
Platt, J. (1981). Evidence and proof in documentary research: 1 some specific problems of documentary research. *Sociological Review*, *29*(1), 31–52. https://doi.org/10.1111/j.1467-954X.1981.tb03021.x
Scott, J. (2014). *A matter of record: Documentary sources in social research*. London: John Wiley & Sons.

Snyder, J. A., & Golladay, K. (2024). More than just a "bad" online experience: Risk factors and characteristics of catfishing fraud victimization. *Deviant Behavior*, 1–21. https://doi.org/10.1080/01639625.2024.2416071

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342–361. https://doi.org/10.1057/s41284-019-00166-w

Steinmetz, K. F., Holt, T. J., & Holt, K. M. (2019). Decoding the binary: Reconsidering the hacker subculture through a gendered lens. *Deviant Behavior*, *41*(8), 936–948. https://doi.org/10.1080/01639625.2019.1596460

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, *15*, 1128–1137. https://doi.org/10.1109/TIFS.2019.2930479

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860–875.

Ugwu, C. (2024). *Nigerian politician arrested in US over $3.3 million romance scam*. Premium times. https://www.premiumtimesng.com/news/headlines/752902-nigerian-politician-arrested-in-us-over-3-3-million-romance-scam.html

Wang, F., & Zhou, X. (2022). Persuasive schemes for financial exploitation in online romance scam: An anatomy on Sha Zhu pan (杀猪盘) in China. *Victims & Offenders*, *18*(5), 915–942. https://doi.org/10.1080/15564886.2022.2051109

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

Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: A serious cybercrime. *Cyberpsychology, Behavior and Social Networking*, *15*(3), 181–184. https://doi.org/10.1089/cyber.2011.0352

Young, M., & Roberts, S. (2021). "Shifting old-fashioned power dynamics"?: women's perspectives on the gender transformational capacity of the dating app, Bumble. *Feminist Media Studies*, *23*(3), 1238–1255. https://doi.org/10.1080/14680777.2021.1992472