International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 2, Mar-Apr 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Yahoo Boys

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The term "Yahoo boys" refers to a group of Internet fraudsters, primarily based in Nigeria and parts of West Africa, who engage in various forms of cybercrime such as advance-fee fraud, romance scams, identity theft, fraud, and business email compromise. This originated from early email scams conducted through Yahoo platforms, which has now evolved into a sophisticated, transnational criminal network leveraging modern technologies including social media, cryptocurrency, and artificial intelligence. Drivers to this phenomenal include factors such as unemployment, poverty, peer influence, and systemic corruption. The global impact of their activities has to do with massive financial losses, emotional harm to victims, and as well as the reputational damage to Nigeria. Overall, the Yahoo boys' phenomenon represents a complex intersection of economic hardship, digital opportunity, and evolving cyber threats, requiring coordinated international and local responses. The paper looks into the legal frameworks and enforcement efforts at combating the cybercrime, cum the challenges posed by technological advancements and adaptive criminal strategies.

KEYWORDS: *Yahoo boys, cybercrime, advance-fee fraud, social media, artificial intelligence, modern technologies, cryptocurrency, unemployment, poverty, peer influence, systemic corruption, reputational damage, international/local responses, legal frameworks, Yahoo-yahoo, motivation, ethics, Nigerian Youth.*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Yahoo Boys" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-2, April 2026, pp.1275-1281, URL: www.ijtsrd.com/papers/ijtsrd101896.pdf

IJTSRD101896

INTRODUCTION

The rapid expansion of the Internet and digital communication technologies has transformed global interaction, commerce, and information exchange. Alongside these advancements has emerged a growing wave of cybercrime, particularly in developing regions where economic challenges and limited regulatory enforcement create fertile ground for digital fraud, such as "Yahoo boys" to strive, as shown in Figure 1. The term "Yahoo boys" is a colloquial expression widely used in Nigeria to describe individuals involved in Internet-based fraud. They are known to perpetrate online scams, including advance-fee fraud (commonly known as "419 scams"), romance scams, identity theft, sextortion, phishing and fake business proposals or email scams (or Business Email Compromise – BEC) – these operations by these scammers, most often involve deceiving victims, who are frequently foreigners, into sending money under false pretenses. The "Beach boys" are known to range from friendly locals to scammers, or young men who hang out on beaches (which are often tourists' areas), or offer services like: surfing/hangout companionship, local tours, souvenir sales, as shown in Figures 2 and 3. The term "419" comes from Nigerian Criminal Code Section 419, which deals with obtaining property under false pretenses [1-4].

HISTORICAL BACKGROUND

The phenomenon known as "Yahoo boys" has its roots in the broader history of fraud in Nigeria, particularly long before the rise of the Internet.

Pre-Internet Fraud (1980s-1990s)

Before digital technology became widespread, fraudulent schemes already was in existence in Nigeria in the form of advance-fee fraud, commonly referred to as "419." This term was from Section 419 of the Nigerian Criminal Code, which criminalizes

obtaining property by false pretenses. These early scams by these scammers were conducted through:

- Postal letters
- Fax messages
- Telephone calls

In this case, the victims were promised large sums of money (e.g., fake contracts or inheritance claims) in exchange for upfront fees.

Emergence of Internet Fraud (Late 1990s-Early 2000s)

The spread of Internet access in Nigeria in the late 1990s made fraudsters/scammers to begin to shift their activities online. Email platforms such as Yahoo became popular tools for sending scam messages, giving rise to the nickname "Yahoo boys." However, during this period:

- Cybercafes became hubs for online activity
- Fraudsters targeted international victims
- Email scams became more sophisticated and widespread

Expansion and Evolution (2000s-2010s)

As technology advanced, so did the methods used by Yahoo boys. Fraud moved beyond email into:

- Social media platforms
- Online dating sites (romance scams)
- Fake business and investment schemes

The use of stolen identities and scripted communication techniques increased, making scams more convincing.

2010s: Yahoo boys diversified their tactics, using social media, WhatsApp, and other platforms.

In recent years, Yahoo boy activities have evolved further with:

- Cryptocurrency-related scams
- Hacking and phishing attacks as shown in Figure 4
- Use of malware and digital tools as shown in Figures 5 and 6.

There has also been a shift toward more organized cybercrime networks rather than isolated individuals.

2015-2020: Government and International Response

The rapid growth of cybercrime has led to stronger enforcement efforts by agencies such as the economic and Financial Crimes Commission (EFCC), established in 2003 to combat financial crimes in Nigeria. While, globally organizations such as the Federal Bureau of Investigation (FBI) and Interpol have collaborated with Nigerian authorities to track and prosecute offenders [5-12]. The National Cyber Crime International Agency (NCCIA) as well assists in combating cyber crime and narcotics control, as shown in Figure 7.

COMMON METHODS USED

Yahoo boys make use of various techniques to manipulate their victims psychologically and financially via:

1. Romance Scams

In this case, these scammers:

- Create fake identities (often attractive profiles) on dating platforms or social media
- Build emotional relationships
- Request money for "emergencies," travel, or medical issues

This is known as the most common tactics globally [13, 14].

2. Business Email Compromise (BEC)

The fraudsters:

- Hack or spoof corporate email accounts
- Impersonate executives or suppliers
- Instruct employees to transfer funds [15, 16].

3. Phishing Attacks: This works by:

- Sending fake emails or messages pretending to be legitimate organizations
- Tricking victims into revealing: passwords, bank details, and personal data.

Examples of this types include: email phishing, SMS phishing ("smishing"), and fake websites [17,18].

4. Advance-Fee Fraud (419 Scam)

- The victim is promised a large sum of money
- The victim may be asked to pay a "processing" or "release" fee
- Fraudster disappears after payment

Some of the examples here are: lottery scams, inheritance claims, and government contract deals [19, 20].

5. Identity Theft & Impersonation

How it works, the fraudsters:

- Steal or fabricate identities
- Pose as: military officers, doctors, or celebrities
- Gain trust and extract money.

Key feature:

- Relies heavily on credibility and trust-building [21].

6. Sextortion: This is a form of blackmail where someone threatens to share nude or sexual images/video of you unless you pay money or do their bidding or do what they want.

How it works:

- Trick victims into sharing intimate content

- Threaten to expose content unless payment is made.

Key feature: This combines sexual exploitation and blackmail [22].

7. Social Engineering ("Client Handling"/Billing)
- This involves the psychological manipulation of victims
- Building trust through: frequent communication, emotional appeal, and persuasion tactics.

Local terms:
- "Client" = victim
- "Billing" = convincing victim to send money [23].

8. "Yahoo Plus" (Spiritual Enhancement Fraud)
This works by:
- Combining cyber fraud with ritual/spiritual practices
- Belief that rituals increases success or influence victims

The key feature is the blending of technology and traditional belief systems [7].

9. Malware & Hacking Tools
It involves the:
- Use of malicious software to: steal data, and monitor activity.
- It includes: keyloggers, and remote access tools

The key feature involves more technical than traditional scams [24].

10. "Bombing" Technique
- This works by sending messages to many potential victims simultaneously
- Lead to increases in chances of success

Key feature: High-volume targeting strategy [25].

11. Violent crimes: When scams fail, the fraudsters may resort to violent crimes like banditry, kidnapping, and ritual killings.

12. Money laundering: In this case, the fraudsters collaborate with Politically Exposed Persons (PEPs) to launder stolen funds into offshore accounts.

LAW ENFORCEMENT EFFORTS

In Nigeria, the Economic and Financial Crimes Commission (EFCC) has arrested and prosecuted several Yahoo boys, with the 2022 report showing a 174% increase in cybercrimes. The EFCC's 2022 crackdown was about the arrest of several Yahoo boys that were involved in romance scams of $60,000 and money laundering. There was also the 2019 case, where a Nigerian man was extradited to the US for a $1 million romance scam. In 2025, EFCC chairman Ola Olukoyede revealed that politically exposed persons (PEPs) were using Yahoo boys to launder billions of naira in stolen funds [26-30].

COMBATING CYBERCRIME IN NIGERIA

Combating cybercrime generally requires a coordinated mix of technology, law enforcement, education, and international cooperation. There is the need to understand cybercrime by all and sundry as illegal activities carried out by the use of computers or the Internet, which includes:
- Hacking and unauthorized access
- Identity theft
- Online fraud and scams
- Malware distribution (viruses, ransomware)
- Cyberstalking and harassment

A foundational concept in cybersecurity is Information Security (IS), which focuses on protecting data confidentiality, integrity, and availability.

Some of the key strategies for combating cybercrime would include:

1. Strong legal frameworks:

In this case, governments are to enact laws to prosecute cybercriminals. A globally recognized treaty is the Budapest Convention on Cybercrime, as shown in Figure 8, which promotes international cooperation and standardizes cybercrime laws. Furthermore, many countries also have national cybersecurity acts and digital protection laws.

2. Law enforcement and intelligence (International collaboration):

Specialized cybercrime units investigate digital offenses. Organizations like INTERPOL and Europol coordinate cross-border operations. Need for collaboration between Nigeria and global law enforcement/extradition treaties and joint investigations.

3. Technological measures and cybersecurity: Organizations and individuals must adopt stronger security systems. Cybersecurity tools help detect and prevent attacks, some of which include:
- Firewalls and intrusion detection systems
- Encryption technologies (based on cryptography)
- Artificial intelligence for threat detection
- Use of multi-factor authentication (MFA)
- Anti-phishing tools and secure payment systems
- AI-driven fraud detection systems by banks and fintech companies.

Companies such as Kaspersky and CrowdStrike are known to have developed cutting-edge solutions.

4. Public awareness and education:

Human error is a major vulnerability. Many victims fall prey due to lack of awareness. Awareness campaigns teach users to:

- Avoid phishing scams – campaigns educating people on identifying scams (fake emails, suspicious links, etc.) can reduce success rates.
- Use strong passwords
- Enable multi-factor authentication
- Digital literacy programs in schools and communities are crucial.

5. International cooperation:

Cybercrime often crosses borders, making collaboration essential. Agencies share intelligence and coordinate operations globally through frameworks like the Budapest Convention.

6. Community and cultural reorientation:

There is a need to address the social acceptance or glamorization of fraud.

- Religious institutions, schools, and media should promote ethical values.
- Public figures discouraging fraud can influence youth behavior.

7. Youth empowerment and employment opportunities:

Unemployment and economic pressure are major drivers of cybercrime. Hence, the need for:

- Providing vocational training, entrepreneurship programs, and job opportunities can reduce incentives to committing cybercrime.
- Encouraging participation in legitimate tech careers (coding, cybersecurity, digital marketing).

ROLE OF ORGANIZATIONS

- Federal Bureau of Investigation (FBI): Tracks cybercriminal networks.
- National Cyber Security Centre (NCSC): Provides guidance and threat intelligence.
- United Nations Office on Drugs and Crime: Supports global cybercrime prevention efforts.

CHALLENGES IN COMBATING CYBERCRIME

Some of these challenges include:

- Rapid technological advancement
- Jurisdictional issues across countries
- Anonymity of attackers
- Shortage of skilled cybersecurity professionals [31-43].

There is the need to protect yourself online by way of:

- Being cautious with personal info: Avoid sharing sensitive details on social media or with strangers.
- Use strong passwords: Combine letters, numbers, and symbols, and update them regularly.
- Enable two-factor auth (2FA): Add an extra layer of security to your accounts. Some popular platforms with 2FA include:
  - Google (Gmail)
  - Facebook
  - Twitter
  - Instagram
  - Banks (check with your provider)
- Verify online relationships: Be wary of those avoiding video calls or meetings [44-46].

CONCLUSION

Yahoo boys' phenomenon is a deeply rooted socio-economic issue, with serious legal consequences, having damaging effect on a country's global reputation such as Nigeria. It tends to also harm victims and communities. It creates a false image of success associated with "Yahoo boys" (such as the riding of flashy cars, luxury items, social media displays) but hides the risks, instability, and legal dangers behind such life style. The bottom line is that "Yahoo boy" culture is not just a crime issue – but borders on serious ethical, social, economic, and global consequences (i.e., it is both a criminal issue and a socio-economic problem). Long-term solutions will require a mix of stricter enforcement, better economic opportunities, education, and a shift in societal values toward legitimate success. More information on Yahoo Boys can be obtained in books in [47-55] and the following related journals:

International Journal of Cyber Criminology

Journal of Financial Crime

African Journal of Criminology and Justice Studies

Mkar Journal of Management and Social Sciences

Journal: Discover Psychology (Springer 2025)

National Journal of Cyber Security Law

Journal: Deviant Behavior (2023)

Journal: Informasi (2025)

International Journal of Law, Crime and Justice

Journal of Asian and African Studies

Sabinet African Journals

Journal of Digital Forensics

REFERENCES

[1] L. Felner (July 24, 2024), "Meta cracks down on 'Yahoo Boys' and thousands of sextortion accounts," https://www.theverge.com/

[2] M. Douet, "Inside the world of the Yahoo Boys, Africa's most infamous romance scammers," https://www.lemonde.fr/le-monde-

africa/inside-the-world-of-the-yahoo-boys-africa's-most-ionfamous-romance-scammers

[3] E. Ukanwa (21 February 2025), "Breaking: EFCC returns over $120,000, =N=70 million to foreign victims defrauded by 'Yahoo Boys.' " https://www.legit

[4] A. M. Auwal & S. Lazarus (2025), "Study on cybercrime victims in Nigeria."

[5] A. M. Auwal & S. Lazarus (2025), *Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria,* Discover Psychology, vol. 5, no. 161.

[6] B. T. Ogundele et al. (2023), "*Cybercrime activities and the emergence of Yahoo Boys in Nigeria," International Conference on Cyber Management and Engineering.*

[7] O. Tade (2013), "*A spiritual dimension to cybercrime in Nigeria: The "Yahoo Plus" phenomenon*," *Human Affairs*.

[8] R. A. Aborisade (2023), "*Yahoo Boys, Yahoo Parents? Parents' disposition towards children's involvement in cybercrimes*," *Deviant Behavior*, vol. 44, no. 7, pp. 1102-1120.

[9] L. I. Akogwo (2018), *The Internet and emergence of Yahoo-Boys Sub-Culture in Nigeria,* International Journal of Cyber Criminology.

[10] A. I. Adeniran (2008), The Internet and emergence of Yahooboys sub-culture in Nigeria, Journal of Cyber Criminology, vol. 12, no. 2, pp. 368-381.

[11] U. A. Ojedokun & M. C. Eraye (2012), Socioeconomic lifestyle of the yahoo-boys: A study of perceptions of university students in Nigeria, International Journal of Cyber Criminology, vol. 6, no. 2, pp, 1001-1013.

[12] O. Tade & U. A. Ojedokun (2012), Perceptions of the police and crime reporting in Nigeria, International Journal of Criminology and Sociological Theory, vol. 1, no. 1, pp. 1-13.

[13] S. Lazarus, M. Button & A. Adogame (2022 October 18), Advantageous comparison: Using Twitter responses to understand similarities between cybercriminals ("Yahoo Boys") and politicians (Yahoo men"), Heliyon, vol. 8, no. 11, e11142.

[14] M. T Whitty (2015), *Mass-marketing fraud in cyberspace*.

[15] E. R. Leukfeldt (2014), *Cybercrime and social engineering*.

[16] M. Button et al. (2014), *Online frauds*.

[17] T. N. Jagatic et al. (2007), *Social phishing*.

[18] C. Cross (2018), *Cybercrime and digital forensics.*

[19] R. G, Smith (2007), *An empirical study of advance fee fraud*.

[20] Nigerian Criminal Code (Section 419).

[21] T. J. Holt & A. M. Bossler (2016), *Cybercrime in progress*.

[22] Europol (2020), *Internet Organized Crime Threat Assessment*.

[23] O. Tade & I. Aliyu (2011), *Social organization of Internet fraudsters in Nigeria*.

[24] *D.* S. Wall (2007), Cybercrime: *The transformation of crime*.

[25] C. K. Orji (2024), *Understanding the crime-grid of the Nigerian Yahoo Boys*, National Journal of Cyber security Law, vol. 7, no.2.

[26] L. Jannamike, "Politicians now launder billions through Yahoo boys – EFCC," https://www.vanguardngr.com/politicians-now-launder-billions-through-yahoo-boys

[27] A. Sulaimon (June 16, 2025), "Yahoo-Yahoo boys bringing national shame to Nigeria – EFCC boss," https://www.punchng.com/yahoo-yahoo-boys-bringing-national-shame-to-nigeria

[28] K. Kasali (June 16, 2025), "Yahoo boys now fueling banditry, kidnapping, others – EFCC," https://www.tvcnews.tv/yahoo-boys-now-fuelling-banditry-kidnapping-others

[29] U. A. Ojedokun & A. A. Ilori (June 2021), "Techniques and underground networks of yahoo-Boys in Ibadan city," International Journal of Criminal Justice, vol. 3, pp. 1-24, https://www.researchgate.net/techniques-and-underground-networks-of-yahoo-boys-in-ibadan-city

[30] "Cybercrime/Yahoo boys scammers dabble in dark magic," https://enactafrica.org/yahoo-boys-scammers-dabble-in-dark-magic

[31] Council of Europe (2001), *Convention on Cybercrime (Budapest Convention).*

[32] INTERPOL, Cybercrime Programme Reports.

[33] Europol, *Internet organized Crime Threat Assessment* (IOCTA).

[34] United Nations Office on Drugs and Crime, Cybercrime publications.

[35] National Institute of Standards and Technology, *Cybersecurity Framework*.

[36] National Information Technology Development Agency (NITDA) promotes cybersecurity awareness.

[37] NITDA (2020), *National Digital Literacy Framework*.

[38] World Bank (2020), Nigeria Digital Economy Diagnostic Report.

[39] United Nations Office on Drugs and Crime (2013), *Comprehensive Study on Cybercrime*.

[40] International Telecommunication Union (2021), *Global Cybersecurity Index*.

[41] Transparency International (2019), *Corruption Perception Index*.

[42] INTERPOL cybercrime initiatives.

[43] UNODC reports on international cybercrime cooperation.

[44] "How two-factor authentication works on Facebook," https://www.facebook.com

[45] "Using an app for two-factor authentication on Facebook," https://www.facebook.com

[46] Facebook Help Center: "Two-factor authentication."

[47] O. Oluku & F. I. Ofili (2025), "Economic livelihood and cyber fraud: A study of the motivations, income and expenditure patterns of Yahoo Boys in Oghara, Delta State," *Mkar Journal of Management and Social Sciences, vol. 7, no. 1.*

[48] T. O. Kolawole et al. (2019), "*Current trend and perception of cybercrime: A study of Yahoo-Yahoo practice in Nigeria," International Journal of Intellectual Discourse.*

[49] M. Bada & J. Nurse (2021), "Profiling the cybercriminal."

[50] N. O. Emmanuel & S. Ameh (2025), "Yahoo Boys vs. Crypto Bros: algorithmic amplification patterns of financial fraud, *Informasi Journal.*

[51] S. O. Adejoh et al. (2019), *"Yahoo boys" phenomenon in Lagos metropolis: A qualitative investigation.*

[52] S. S. Evans-Ibe, "Bombing, billing, and cash-out: the dynamics of the illicit flow of money through international cyber fraud by Nigerian "Yahoo Boys," https://www.journalasap.org

[53] O. P. C. Wariboko & F. C. Nwanyanwu (September 10m 2024), "The dark side of connectivity: A socio-ethical exploration of Internet fraud and Nigerian Youth," Agidigbo: ABUAD Journal of the Humanities, vol. 12, no. 1, pp. 89-104. https://www.journals.abuad.edu.ng

[54] *A.* Oyenuga & A. Aderinto (2018), "Identity, recruitment and initiation of youth into cybercrime in metropolitan Lagos," XIX ISA World Congress of Sociology, July 15-21, 2018.

[55] Oyenuga, "Youth and cybercrime subculture in Lagos State, Nigeria," University of Ibadan, Nigeria, 2017.

Figure 1. cybercrime
Source: https://en.wikipedia.org/wiki/Cybercrime

Figure 2. The Beach boys
Source:
https://en.wikipedia.org/wiki/The_Beach_Boys

figure 3. List of cybercriminals
Source:
https://en.wikipedia.org/wiki/List_of_cybercriminals

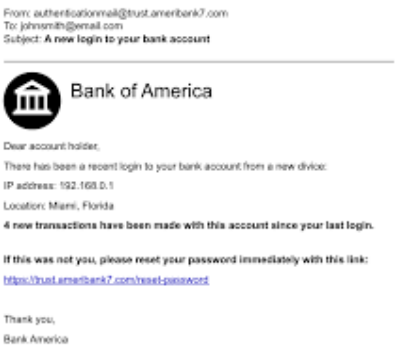

Figure 4. Phishing
Source: https://en.wikipedia.org/wiki/Phishing

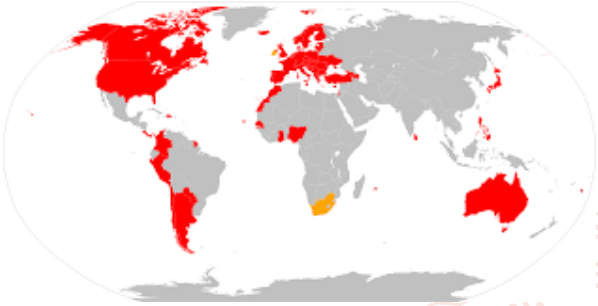

Figure 5. Budapest Convention on cybercrime
Source:
https://en.wikipedia.org/wiki/Budapest_Convention_on_Cybercrime

Figure 6. Antivirus software
Source:
https://en.wikipedia.org/wiki/Antivirus_software

Figure 7. Malware
Source: https://simple.wikipedia.org/wiki/Malware

Figure 8. National Cyber Crimes Investigation Agency
Source:
https://en.wikipedia.org/wiki/National_Cyber_Crimes_Investigation_Agency