UKR Journal of Arts, Humanities and Social Sciences (UKRJAHSS)
Homepage: https://ukrpublisher.com/ukrjahss/
Email: submit.ukrpublisher@gmail.com
Volume 2, Issue 8, 2026
ISSN: 3107-359X (Online)

Behavioural and Socioeconomic Profiles of Cybercrime Offenders: Implications for Cybersecurity in Anambra State Correctional Centres

Yadilichukwu Triumphant Ikwuadinso[1] & Victor Ilozue[2]

Department of Criminology and Security Studies, Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State, Nigeria

***Corresponding Author**: Yadilichukwu Triumphant Ikwuadinso

DOI: *https://doi.org/10.5281/zenodo.22048281*

Article History

Original Research Article

Received: 18-06-2026

Accepted: 25-07-2026

Published: 21-08-2026

Citation: Yadilichukwu Ikwuadinso, & Victor Ilozue. (2026). Behavioural and socioeconomic profiles of cybercrime offenders: Implications for cybersecurity in Anambra State correctional centres. UKR Journal of Arts, Humanities and Social Sciences, 2(8), 152-166.

Abstract

The rise of internet fraud, popularly called "yahoo-yahoo," among youths remains a major security challenge in Nigeria. While many studies interview free students on campus, very little is known about the profiles of fraudsters who have been caught and convicted. This study examines the behavioral and socioeconomic profiles of cybercrime offenders and their implications for cybersecurity in correctional centers within Anambra State. Adopting a descriptive documentary research design, the study integrated qualitative interview evidence from 10 inmates with quantitative survey data from 443 retrieved questionnaires across selected custodial facilities. The findings reveal that cybercrime in this context is not a single form of offense. General online fraud emerged as the most common crime type (65.2%), followed closely by phishing (48.3%) and identity theft (39.7%), while high-level technical hacking was much lower (27.3%). Key behavioral and socioeconomic drivers included the strong belief that police would never catch them (66.4%), peer pressure from friends (58.5%), and family poverty (39.1%). Statistically, the study established significant positive relationships between cybercrime typologies and profiling accuracy ($r = .612$, $p < .001$), and between cybersecurity effectiveness and profiling accuracy ($r = .584$, $p < .001$). Crucially, the data exposes a serious gap between prison punishment and real reform; while 88.9% of inmates confirmed that phones and internet are strictly banned, only 41.3% had ever participated in any positive computer or ICT rehabilitation program. This remains a major missed opportunity as 64.8% of the inmates expressed a strong willingness to drop internet fraud and turn their digital skills toward legal IT employment. The study concludes that the Nigerian Correctional Service (NCoS) must move past simple device bans. Effective prison security must be combined with monitored computer workshops, psychological counseling against the "get-rich-quick" mindset, and structured post-release support to permanently stop these youths from returning to digital fraud.

Keywords: *Cybercrime, Offender Profiling, Correctional Centers, Rehabilitation, Anambra State, Yahoo-Yahoo.*

1. Introduction

The rapid development of modern technology has transformed the way crimes are committed around the world. Nowadays, financial transactions, social relations, education, business, and even government operations rely heavily on online communications. This change has opened up new opportunities for development, but on the other hand, it has also given criminals new tools to deceive people, steal personal information, forge identities, and transfer illegal funds. As a result, cybercrime has moved beyond the previously held notion of the work of a solitary hacker; it now includes a wide range of crimes that rely on or benefit from technology (Bada & Nurse, 2021; Edwards et al., 2022; Peersman et al., 2022).

This changing nature of cybercrime has made the study of the behavior of its perpetrators a major issue. Bada and Nurse (2021), in their study of the history of cybercriminal profiling, state that there is still no single, universally accepted definition of cybercriminals. Most existing

research has focused on "hackers," even though cybercrime involves a diverse group of individuals with varying degrees of computer knowledge, goals, and methods of operation. Edwards et al. (2022) also support this view, describing cybercriminals as a diverse group of individuals whose behaviors vary depending on the type of crime they commit, their level of computer knowledge, and their motivations. This has a direct impact on legal practice: it should not be assumed that a person convicted of cybercrime has the same behavior or knowledge of the machine as a person who creates malware or accesses confidential information systems without authorization.

In the Nigerian context, this distinction is of great importance. Internet fraud (i.e. Yahoo-Yahoo) has become one of the most prevalent crimes in the country, especially among the youth. Experts in Nigeria have linked this to a number of factors such as peer pressure, economic hardship, the desire to make a name for themselves, learning from society, and how young people view the benefits or consequences of crime (Orjiakor et al., 2022; Obianagwa et al., 2023; Uchime et al., 2024). Importantly, these data do not suggest that unemployment or poverty is the sole driver of cybercrime. However, social and economic factors that influence the mindset and behavior of individuals make online money-making opportunities more attractive to some.

One of the most useful contributions in this area comes from Orjiakor et al. (2022), who examined the psychological strategies of online fraudsters in Nigeria. Their specific study of 12 young men involved in fraud schemes—including one who was in prison—found that peer influence was a major factor in their involvement. They also identified the psychological strategies of neutralization, entitlement, minimization, and rationalization in their narratives. The significance of this research lies in the fact that it is not just the pursuit of money that drives people to commit online crimes, but also the mental processes that make the crime seem justified in the mind of the perpetrator.

Moreover, the influence of peers is increasingly evident in research conducted in Anambra State. Onwuchekwe et al. (2025), in their study of youth in Onitsha North Local Government Area, examined how peer pressure influences involvement in cybercrime. Their findings are highly relevant to this work as Onitsha is one of the major commercial and urban centres of the state. The study's focus on peer relationships, unemployment, and cybercrime among youth supports the argument that crime cannot be understood solely in terms of individual technology.

The economic aspect should also be given equal attention. Obianagwa et al. (2023) studied youth unemployment and cybercrime in Nigeria, where they found that the problem of long-term unemployment contributes to the fueling of cybercrime in the country. This finding is consistent with the general idea that when legitimate sources of income are scarce, illicit activities become attractive to some youth. Uchime et al. (2024) also identified youth unemployment, poverty, generational effects, increased internet access, and technological advancement as factors associated with the persistence of cybercrime among Nigerian youth.

However, relying on economic factors alone will not translate into anything. There are many unemployed Nigerian youth who do not engage in cybercrime. Similarly, not everyone who is financially strapped turns to crime. Therefore, economic conditions must be viewed in conjunction with opportunities, relationships, perceptions, and perceived rewards. This position is supported by research examining the psychological and social context of cybercriminals. For example, Palmieri et al. (2021) found that personality traits can contribute to differences in how people are inclined to engage in online crime. Their study suggests that individual differences are important even in a technology-driven environment.

Social context is important for cybercrime in Nigeria because crime can be learned through social interactions. Youth can learn tactics, diversion, victim recognition, and avoidance strategies from their peers or experienced criminals. Orjiakor et al. (2022) found that most respondents identified friends as the main channel through which youth engage in cybercrime. Research on global cybercrime networks also suggests that criminals operate in a networked system where they share knowledge, resources, and opportunities to commit crimes (Campobasso et al., 2023).

This changing climate of cybercrime means that correctional facilities must rethink their definition of security. Traditional prison security focuses on escapes, violence, the introduction of illegal substances, and disorder. These factors are important, but modern technology presents a new challenge to the security of institutions. A prisoner with advanced computer skills may pose a different threat than a prisoner whose crime is based solely on verbal deception. This threat can extend beyond the prison walls, especially if offenders continue to communicate with outside organizations or attempt to use secret communication channels.

Therefore, offender profiling can be an important bridge between criminology and cybersecurity. However, this work must be conducted with caution. Bada and Nurse (2021) note the lack of consistency in the definition and research methods in the work related to cyber-offender profiling. Petherick and Brooks (2020) also caution that offender profiling should identify evidence rather than relying on stereotypes or unfounded assumptions. In

correctional facilities, the lack of accurate profiling can lead to two problems at once: high-risk individuals may be left unattended, while individuals with only basic computer skills may be subject to unnecessary sanctions.

Behavioral rehabilitation programs are also effective. Cybercriminals often have skills that they can use for legitimate activities. Simply suppressing their computer knowledge without providing them with alternative opportunities may leave the root cause of the problem unaddressed. Lim and Thing (2022) emphasize the need for behavioral rehabilitation programs that consider the factors that drive cybercriminals to commit crimes, the pathways they take, and their opportunities for reintegration into society. This is especially important in a country where computer knowledge is increasingly integrated into jobs, businesses, and the wider economy.

The problem of recidivism reinforces the argument for rehabilitation. Scholarly studies of Nigerian correctional facilities have consistently shown that inadequate rehabilitation, weak reintegration systems, poor post-release support, and staffing constraints are factors that make successful post-prison reintegration difficult (Omoruyi & Ego, 2023; Irogbo, 2024; Ilori, 2024). Omoruyi and Ego (2023), using secondary exit data, directly linked inadequate rehabilitation and poor reintegration to the challenges faced by former prisoners after release.

For cybercriminals, these problems can be very serious. A person who turns to cybercrime due to unemployment, peer pressure, and the desire to make a quick buck may fall back into the same social and economic situation they left behind after serving their prison sentence. If rehabilitation programs do not change the offender's mindset, and there is no permanent employment opportunity available, then sending them to prison will only serve to temporarily suspend the crime, without addressing the underlying causes that led to it in the first place.

Consequently, this article examines the issue of profiling cybercriminals from the perspective of cyber security in correctional facilities. The article argues that improving security should not be limited to restricting devices or computer systems. Instead, it should include understanding the offender's behavior, their technological capabilities, their economic situation, the friends they interact with, and the type of behavioral modification they need.

This paper is guided by four clear objectives. First, it measures the prevalence and types of recorded cybercrimes affecting offenders in Anambra State correctional facilities. Second, it examines the behavioral and economic characteristics of cybercriminals, and the implications for improving security in correctional facilities. Third, it examines the relationship between cybercrime patterns, the quality of offender profiling, and the impact of cybercrime safety in the correctional system. Fourth, it assesses the effectiveness of current cybercrime and correctional facility security laws and policies in reducing the risk of recidivism among registered offenders.

This article contributes to the field of knowledge in two important ways. The first is that it brings together behavioral and economic data, which are often examined separately by scholars. The second is that it links offender profiling directly to the cyber security of correctional facilities, rather than treating cybercrime as a policing or victim protection function. The choice of Anambra State as the study site is deliberate. Although scholarly research on cybercrime in Nigeria is increasing, research linking offender profiles, correctional facility management, and cyber security, particularly in Anambra State, is still very limited.

2. Literature Review

Cybercrime as a Heterogeneous Form of Criminality

Cybercrime is not a single, well-defined phenomenon. It encompasses activities that target, exploit, or facilitate the use of technology to commit crimes. This distinction is important because each cybercrime requires a combination of computer science, social skills, goals, and capabilities. Bada and Nurse (2021) reviewed research on cybercriminal profiling and found that the field is still fragmented. Their study identified 39 relevant activities and showed that researchers often focus on hackers while not fully understanding other groups of cybercriminals. They concluded that the lack of a single, standardized approach to profiling makes it difficult to provide a comprehensive profile of a cybercriminal.

Edwards et al. (2022) also highlight the diverse characteristics of cybercriminals. Their study of highly technology-dependent offenders found differences in their motivations, characteristics, and capabilities in the field of technology. The implication is that the term “cybercriminal” should be viewed as a broad term that encompasses many things rather than a specific mental illness. Peersman et al. (2022) further examine financial cybercriminals and argue that understanding the characteristics and motivations of the offender can help cybercriminals develop treatment strategies that are appropriate for both the social and technological contexts. The relevance of this to correctional facilities is clear; if offenders vary in motivations and capabilities, then treatment measures should also vary rather than a one-size-fits-all approach.

Major Cybercrime Typologies

Scholarly studies in Nigeria consistently identify online financial fraud as a major form of technology-enabled crime. This includes advance-fee fraud, romance scams, phishing, impersonation, identity theft, and related forms of online fraud. These forms are not static; as internet use, digital platforms and financial technologies evolve, offenders also adapt their methods. A recent review of cybercrime and cyber policy in West Africa highlights the rapid development of cybercrime alongside challenges in legal and institutional responses (Adewopo et al., 2025). Research in Nigeria has also linked online fraud among young people to economic pressures, social influences and weaknesses in prevention and security responses (Okeke & Onyekachukwu, 2024; Sani et al., 2024; Uchime et al., 2024). International research further shows that cybercrime may involve both individual actors and organized networks with different levels of expertise and capability (Campobasso et al., 2023; Europol, 2024).

Uchime et al. (2024) argue that the increased availability of smartphones, laptops, and the internet has expanded the scope for cybercrime, while weak law enforcement has limited protection. Their study is useful because it moves the conversation away from criminals and examines the institutional context that enables cybercrime to persist. International research also shows that cybercrime is increasingly associated with specific activities for individuals. Campobasso et al. (2023) examined cybercrime networks and demonstrated how criminal networks can facilitate the exchange of knowledge, services, and opportunities. This finding is relevant to the design of offender profiles because an individual's place in the cybercrime system may not be clear based on the type of crime they commit. For correctional facilities, this means that inmates need to be assessed according to their involvement in cybercrime. A social engineer, a fraud facilitator, a credit card fraudster, and a skilled hacker may each require different types of treatment and behavior modification.

Behavioral Characteristics of Cybercrime Offenders

Behavior is central to the development of criminal profiling. However, scholarly studies do not support the idea that cybercriminals have a single, unique behavioral profile. Instead, distinct behavioral patterns emerge across different groups. Bada and Nurse (2021) note that behavioral patterns are still an underdeveloped area of research in cybercriminal profiling. Edwards et al. (2022) also find that current evidence suggests multiple offender profiles rather than a single, well-defined profile.

Palmieri et al. (2021) provide empirical evidence by examining the nature and propensity to engage in online delinquency using Reinforcement Sensitivity Theory. Their findings suggest that differences in temperament may help explain why some individuals are more prone to online delinquent behaviors than others. This does not mean that temperament should be used to label individuals as criminals. Instead, temperament measures should examine the broad range of traits associated with delinquency, including risk-taking, impulsiveness, novelty seeking, attentional bias, objectification, views of authority, and perceptions of victims.

Evidence from Nigeria paints a very clear picture. Orjiakor et al. (2022) found that cybercriminals described cognitive self-defense strategies, feelings of entitlement, minimizing the seriousness of the crime, and providing false evidence. Some participants developed narratives that shifted responsibility for the crime away from themselves and towards the broader social or political context. These findings are important for prison reform. If crime is fueled by the belief that victims are responsible for allowing themselves to be deceived, then providing technical training alone will not address the risk. An offender may leave prison with improved technical knowledge but no change in their mindset about committing the crime.

Peer Influence and Social Learning

The influence of peers is a recurring theme in research on cybercrime. The online environment can facilitate learning because people can access knowledge through friends, online groups, and social media. Orjiakor et al. (2022) found that peers are a major source of exposure to cybercrime among Nigerian youth. Participants in their study described a social environment where fraud can be introduced, reinforced, and normalized. This suggests that cybercrime can be learned socially rather than being viewed as an individual choice.

A recent study by Onwuchekwe et al. (2025) is particularly relevant to this article as it examined peer pressure and involvement in cybercrime in Onitsha North Local Government Area of Anambra State. Its focus on the relationship between peer pressure and youth involvement provides strong empirical evidence that supports other scholarly writings on social influence. Campobasso et al. (2023) extend this evidence beyond traditional peer groups by showing how secret online groups facilitate communication among criminals. Such groups can make machine learning, criminal activities, and partners more readily available.

The implications of this for correctional facilities are complex. The prison environment may discourage some external criminal contacts, but it can also provide opportunities for like-minded offenders to communicate with each other. Therefore, the correctional facility needs

to distinguish between social interactions that support correction and interactions that encourage learning to engage in criminal behavior.

Pro-Criminal Cognition and Rationalization

One of the main themes that emerges from scholarly research in Nigeria is the role of psychological justification in criminal defense. Orjiakor et al. (2022) found that criminals use a variety of false justifications to explain or defend their actions. These include minimizing the harm they cause, feeling entitled to the money, deflecting responsibility for the crime, and viewing cybercrime in the context of everyday social problems. This is important because it challenges the common assumption that criminals necessarily view their behavior as wrong. Some may recognize that the law prohibits fraud but still believe that their actions are rational or justified.

Such thinking can affect the outcome of correctional programs in prison. An offender who believes that cybercrime is harmful may respond differently to correctional programs than one who continues to view crime as a means of escape or a positive step towards addressing social injustice. This is where cognitive and behavioral interventions become important. Correctional programs in prison should provide opportunities for offenders to examine the consequences of their behavior, understand the pain that victims feel, challenge their false beliefs, and provide alternative ways to cope with economic or social pressures.

Socioeconomic Characteristics

Economic and social conditions are among the frequently cited factors associated with cybercrime in Nigeria, with youth unemployment receiving particular attention. Obianagwa et al. (2023) examined the relationship between youth unemployment and cybercrime using historical and time-series evidence and concluded that persistent unemployment contributes to the growth of cybercrime. Uchime et al. (2024) likewise associated unemployment, poverty, peer pressure and increased access to technology with cybercrime among Nigerian youth. The National Bureau of Statistics (2024) provides official labour-force evidence on employment and unemployment conditions in Nigeria, while the World Bank (2024) reports continuing short-term pressures on households and businesses alongside structural challenges to growth and job creation. These sources provide important socioeconomic context, although they do not establish that unemployment or economic hardship automatically produces cyber offending. Rather, economic pressures appear to interact with social relationships, opportunities, perceived rewards and individual decision-making (Obianagwa et al., 2023; Onyeachu et al., 2025; Uchime et al., 2024; Willie et al., 2022).

Willie et al. (2022) also examined unemployment and cybercrime among Nigerian youth, linking economic conditions and pressure to migrate abroad to the rise of money-making cybercrime. However, economic hardship should not be taken as a sole explanation. Many Nigerians experience unemployment or financial hardship without engaging in cybercrime. Therefore, a more plausible explanation is that of a combination of factors; economic hardship may be a driving force or a weakness, but the influence of peers, opportunities, opinions, and perceived rewards also contribute to determining whether an individual will turn to crime.

Material Aspirations and Relative Deprivation

The pursuit of material possessions is closely linked to economic and social factors. The appeal of cybercrime is not necessarily limited to meeting everyday needs; status, perceived financial success and the desire for rapid upward mobility may also shape motivations. Young people may compare themselves with peers who display expensive clothing, cars, phones, travel and other symbols of success. Where legitimate routes to such status appear slow or inaccessible, cybercrime may become an attractive shortcut for some individuals. Nigerian research links cybercrime among young people to perceived economic opportunities, peer influence and socio-economic pressures (Orjiakor et al., 2022; Onyeachu et al., 2025). The implication is that a socioeconomic profile of cyber-offenders should include more than income or employment status. It should also consider aspirations, perceived inequality, peer comparisons and expectations about economic mobility.

This interpretation is consistent with the findings of Orjiakor et al. (2022), where participants used socio-economic factors to predict cybercrime. It is also consistent with a study of university students in Nigeria, where peer influence and perceived financial success were found to be factors that encourage cybercrime. The key point here is that profiling the socio-economic profile of a cybercriminal should include more than just income or employment status. It should consider life aspirations, perceived inequality, comparisons to others, and expectations about changing economic conditions.

Age and Gender

The scholarly literature generally highlights the significant contribution of young males to cybercrime groups in Nigeria. Orjiakor et al. (2022), for example, studied young male cybercriminals and found the influence of peers and perceived support for crime among those surveyed. However, gender and age should be interpreted with caution. The fact that men are more likely to be involved in

cybercrime does not mean that women are not involved in cybercrime, nor does being younger mean that criminal behavior is less likely. Demographic characteristics are useful for understanding the structure of a group of people, not for assessing individual criminality or risk. Edwards et al. (2022) explicitly caution against making generalizations by highlighting the different characteristics of cybercrime groups. Therefore, a good correctional system is one that combines demographic data with behavioral, technical, and brief descriptions of the crime committed.

Digital Competence and Offender Capability

Digital and technical competence is an important aspect of cybercrime profiling. There is a tendency to assume that all cybercriminals are highly skilled in technical fields, but evidence suggests otherwise. Some forms of cybercrime require advanced technical knowledge, while others depend more heavily on social engineering, manipulation, communication skills, or readily available tools. Peersman et al. (2022) note that financially motivated cybercrime can involve varying levels of technical ability and different goals, while Bada and Nurse (2021) show that cyber-offender profiles differ considerably across offence types and levels of expertise.

This distinction is important for correctional security. A person who uses social engineering or verbal deception poses a different technical risk from an offender who has the ability to penetrate, manipulate, or damage computer systems. Both may fall within the broad category of cyber-offenders, but the cybersecurity measures required to manage them are not identical. Therefore, offender assessment should record the nature of previous online activities, the strategies used, the level of digital competence, and the technical skills that remain relevant. Such an approach is consistent with the evidence that cybercriminal populations are heterogeneous and should not be treated as a single offender type (Bada & Nurse, 2021; Edwards et al., 2022; Peersman et al., 2022).

Theoretical Explanation of Cybercrime Behaviour

Three criminological theories are particularly useful for interpreting the behavioural and situational dimensions of cybercrime: Social Learning Theory, Rational Choice Theory, and Routine Activity Theory. Social Learning Theory explains how criminal attitudes and techniques may be acquired and reinforced through interaction with peers and significant others (Akers, 1998). In the Nigerian context, the findings of Orjiakor et al. (2022) and Onwuchekwe et al. (2025) provide empirical support for examining peer influence, social reinforcement, and the normalization of cybercrime among young people.

Rational Choice Theory helps explain why an individual may choose cybercrime after assessing expected rewards, risks, effort, and available opportunities. Cornish and Clarke (1986) conceptualize offending as a form of decision-making in which offenders make choices within specific situations and under conditions of bounded rationality. This perspective is relevant to financially motivated cybercrime because offenders may perceive substantial rewards while believing that the risks of detection or victim retaliation are comparatively low. Peersman et al. (2022) similarly identify motivations and perceived opportunities as important to understanding financially motivated cyber offending. Routine Activity Theory, developed by Cohen and Felson (1979), focuses on the convergence of a motivated offender, a suitable target, and the absence of capable guardianship. In cybercrime, this perspective draws attention to the availability and accessibility of targets and weaknesses in protective arrangements. In a correctional setting, potential targets may include administrative information systems, staff accounts, communication technologies, and other digitally connected resources. The three theories therefore complement one another: Social Learning Theory explains how cybercriminal attitudes and techniques may be learned, Rational Choice Theory explains how offending decisions may be shaped by perceived costs and benefits, and Routine Activity Theory explains how opportunities arise when suitable targets and weak guardianship converge (Akers, 1998; Cohen & Felson, 1979; Cornish & Clarke, 1986).

Offender Profiling and Profiling Accuracy

Criminal profiling is useful for prison security, but it must be based on sound research. Bada and Nurse (2021) found significant inconsistencies in research on cybercrime profiling, suggesting that the field remains methodologically fragmented. Petherick and Brooks (2020) similarly argue that profiling should be grounded in evidence rather than unfounded assumptions. Profiling based solely on age, gender, appearance, device ownership, or other superficial characteristics can therefore be misleading. For correctional purposes, profiling should incorporate offence type, level of digital competence, behavioural beliefs, prior offending, relevant social relationships, socioeconomic circumstances, participation in correctional programmes, and release plans. Portela et al. (2024) provide evidence that algorithm-supported decision-making can improve the accuracy of risk assessment, while also highlighting the continuing importance of human judgement and oversight. Their findings are relevant because risk assessment in correctional facilities should support, rather than replace, trained professional decision-making.

Cybersecurity in Correctional Institutions

Cybersecurity in correctional institutions requires attention because modern custodial systems increasingly depend on

digital information, communications and connected technologies. Contemporary cybersecurity assessments show that cyber threats involve a broad range of actors, techniques and targets, with ransomware, attacks against data and services, online fraud, and other forms of malicious activity remaining significant concerns (European Union Agency for Cybersecurity [ENISA], 2024; Europol, 2024; International Telecommunication Union [ITU], 2024). INTERPOL's African Cyberthreat Assessment Report also identifies online scams, business email compromise, ransomware and social-engineering techniques among important threats affecting the African cyber environment (INTERPOL, 2024). These developments are relevant to correctional institutions because administrative databases, staff accounts, communication systems, surveillance technologies and other connected resources can become security targets where access controls and guardianship are weak.

The security problem is therefore twofold. Correctional institutions must prevent unauthorized access, manipulation, disclosure or disruption of their digital systems while also allowing technology to support legitimate education, administration and rehabilitation. A blanket prohibition on technology may reduce some immediate risks but can also undermine legitimate correctional and reintegration activities. Conversely, unrestricted access can create avoidable exposure to cyber threats. The World Economic Forum (2025) emphasizes the growing complexity of the cybersecurity environment, while the ITU (2024) stresses the continuing need for stronger national and institutional cybersecurity action. A risk-based approach is therefore more appropriate, with access to devices, networks and digital resources determined by assessed need and risk. Such controls may include segmented or isolated systems, restricted communications, monitored devices, authentication controls, staff training, incident-response procedures and explicit authorization for higher-risk digital activities (ENISA, 2024; Europol, 2024; INTERPOL, 2024; ITU, 2024; World Economic Forum, 2025).

Rehabilitation, Reintegration and Recidivism

Correctional services are central to the rehabilitation and reintegration dimensions of this paper. If offender profiling is limited to identifying individuals who should be restricted from technology, profiling becomes a monitoring tool rather than a criminological strategy for correctional intervention. Omoruyi and Ego (2023) found that inadequate rehabilitation and poor post-release support contribute to difficulties in reintegration and recidivism in Nigerian custodial centres. Irogbo (2024) similarly identified inadequate facilities, staff-training problems and weak post-release support as challenges to effective rehabilitation, while Ilori (2024) emphasized social and economic reintegration in addressing recidivism. These findings have particular implications for cyber-offenders because technical skills may remain useful after release, but their application depends partly on legitimate opportunities and social conditions. Economic pressures and limited employment opportunities can form part of the environment to which an offender returns (National Bureau of Statistics, 2024; World Bank, 2024). Accordingly, Lim and Thing (2022) argue that cybercrime intervention should address the factors that drive offending while also providing pathways for reintegration into society.

Digital Skills as a Rehabilitation Opportunity

Technology presents a particular challenge for correctional institutions because the same digital skills that may have been used in cybercrime can also support legitimate employment after release. Lim and Thing (2022) argue that effective cybercrime intervention should address offender motivations and create pathways for reintegration, while Nigerian correctional research highlights the importance of rehabilitation, staff capacity and post-release support (Irogbo, 2024; Omoruyi & Ego, 2023). A viable approach proposed here is supervised technology rehabilitation. Under such a model, offenders could receive controlled training in areas such as computer programming, web design, cybersecurity, data management and other legitimate digital occupations. Training could be delivered on isolated systems without unrestricted access to external networks. Such arrangements would allow correctional institutions to treat digital competence as a rehabilitation resource while maintaining proportionate security controls.

Research Gap

The reviewed literature reveals three major gaps. First, research on cybercrime in Nigeria has largely focused on youth, university students and the general public, while comparatively little published research examines cybercrime in the context of correctional security. Second, behavioural and socioeconomic factors are often examined separately rather than integrated into a single offender-profile framework. Third, there is limited published evidence specifically linking cybercrime profiling to cybersecurity management in correctional institutions in Anambra State. This paper addresses these gaps by bringing together behavioural, social and socioeconomic evidence and translating it into a correctional cybersecurity framework. The reviewed records should not be treated as a direct census of prisoners in Anambra State; rather, they provide an analytical basis for future empirical research in the state's correctional institutions.

3. Methodology

This study adopted a descriptive mixed-method research design to examine the behavioural and socioeconomic profiles of cybercrime offenders and their implications for cybersecurity in Anambra State correctional centres. The quantitative component employed a cross-sectional survey, while qualitative data were obtained through in-depth interviews. The combination of both approaches enabled the study to establish measurable patterns in cybercrime involvement and offender characteristics while also capturing inmates' experiences and perceptions concerning cybercrime, profiling, cybersecurity and rehabilitation.

The study was conducted in two correctional facilities in Anambra State, namely the Onitsha Custodial Centre and the Awka (Amawbia) Correctional Centre. The facilities were purposively selected because they provided appropriate settings for examining inmates involved in cyber-related and technology-enabled offences and the institutional measures used in managing them. The target population comprised inmates in the selected correctional centres, with particular attention to those who had sufficient experience of custodial supervision to provide informed responses. A total of 450 questionnaires were administered, of which 443 were successfully retrieved and found usable for analysis. In addition, 10 inmates were purposively selected for in-depth interviews to provide qualitative evidence on their pathways into cybercrime, motivations, peer influence, technical skills, perceptions of risk, experiences of profiling and rehabilitation.

Data were collected using a researcher-developed questionnaire titled *Interaction between Cyber-Crime, Cyber-Security, and Criminal Profiling among Detained Criminals in Anambra State Correctional Centres (IC³PDAC)* and an in-depth interview guide. The questionnaire covered respondents' demographic characteristics, cybercrime typologies, behavioural and socioeconomic characteristics, criminal profiling, cybersecurity practices and rehabilitation. The instruments were reviewed by experts in criminology, cybersecurity studies, and measurement and evaluation to establish face and content validity. A pilot study involving 20 inmates outside the study area was conducted to assess the clarity and suitability of the questionnaire. Reliability was assessed using the Kuder-Richardson Formula 20 (KR-20), which was considered appropriate for the predominantly categorical and dichotomous items contained in the instrument.

Data collection was carried out with the assistance of four trained research assistants. The questionnaires were administered directly to eligible respondents, while the selected interview participants were engaged separately using the interview guide. Participation was voluntary and respondents were informed of the purpose of the study and the confidentiality of their responses. Completed questionnaires were coded and analyzed using the Statistical Package for the Social Sciences (SPSS), version 23. Descriptive statistics, particularly frequencies and percentages, were used to summarize the data, while Pearson Product-Moment Correlation was employed to test the relationships between cybercrime typologies, cybersecurity efficacy and criminal profiling accuracy at the 0.05 level of significance. The interview responses were analyzed thematically, with attention to recurring issues relating to motivation, peer influence, technical competence, risk perception, profiling, institutional controls and rehabilitation. Findings from both components were integrated during interpretation to provide a broader understanding of the behavioural and socioeconomic profiles of cybercrime offenders in the study area.

4. Results And Discussion Of Findings

To gather facts for this study, the researcher shared a total of 450 questionnaires with the right inmates inside the selected correctional centers. Out of these, 443 questionnaires were successfully collected back and filled properly for analysis. This gives a very high response rate of 98.4%. To get deeper personal stories, the researcher also conducted private, one-on-one interviews with 10 selected inmates. the findings are arranged based on what this project wants to achieve. The numbers from the questionnaires are explained side-by-side with the real words of the inmates and recent studies from top researchers.

Table 1: Prevalent Cybercrime Typologies among Detained Offenders

Cybercrime Typology	Frequency (\(N=443\))	Percentage (%)
Online fraud	289	65.2%
Phishing	214	48.3%
Identity theft	176	39.7%
Hacking	121	27.3%
Cryptocurrency-related offences	98	22.1%

Source: Field Survey, 2026.

The facts in Table 1 reveal that general online fraud is the most common crime among the inmates, with 289 respondents (65.2%) admitting they were jailed for it. Phishing came second with 214 inmates (48.3%), while identity theft followed closely with 176 inmates (39.7%). Advanced computer hacking was reported by 121 respondents (27.3%), and crypto-currency scams were the least common, recorded by 98 inmates (22.1%).

The high number of online fraud cases matches recent reports on how internet theft has spread across southern Nigeria. For instance, Okeke and Onyekachukwu (2024) noted that digital fraud is changing quickly because technology makes it easy for youths to lie to victims online. However, while past studies only guessed these numbers by interviewing free university students, our current finding is unique because it gets these facts straight from convicted criminals who are already inside the cells.

The high percentage of inmates involved in phishing (48.3%) also reveals a big secret. Phishing does not require a person to be a computer genius; it only requires social engineering, fake websites, and the ability to trick emotional human beings. This confirms the warnings by Bada and Nurse (2021) that we must stop looking at all cybercriminals as if they are the same. Some are just smooth-talkers, while others are highly technical. Similarly, Edwards et al. (2022) argued that internet thieves have completely different motivations, computer skills, and criminal habits.

These findings give prison authorities in Anambra State a clear direction for rehabilitation. An inmate who only uses smooth-talking or phishing to steal money needs a completely different counseling and behavior reform program compared to a dangerous hacker who breaks into banks. Therefore, instead of labeling every young inmate generally as a "cybercriminal," the Nigerian Correctional Service (NCoS) must profile each inmate based on their specific skills and crime pathways.

Table 2: Behavioural and Socioeconomic Characteristics of Respondents

Characteristic	Frequency (N=443)	Percentage (%)
Believed low detection risk	294	66.4%
Peer influence (Friends' pressure)	259	58.5%
Advanced digital competence (High IT skills)	207	46.7%
Desire for rapid wealth (Quick money)	202	45.6%
Poverty or financial hardship	173	39.1%

Source: Field Survey, 2026.

The facts in Table 2 show that 46.7% of the inmates had advanced computer and digital skills before the police caught them. Peer pressure from friends was reported by 58.5% of the respondents, while 45.6% admitted that the hunger for quick wealth drove them into the crime. Also, 39.1% of the inmates blamed poverty and family financial problems for their choices. Most importantly, a huge majority of the inmates (66.4%) strongly believed before their arrest that the police or EFCC would never catch them.

Peer influence stands out as one of the biggest reasons why young people join cybercrime networks. This finding directly matches the study of Orjiakor et al. (2022), who discovered that Nigerian internet fraudsters rely on their friends to learn the trade, and they use different mental excuses to make their bad behavior look acceptable. This also agrees with what Onwuchekwe et al. (2025) found in Onitsha North, Anambra State, where there is a strong link between bad peer groups and youth cyber-fraud.

This situation fits perfectly into Social Learning Theory, which teaches that people copy bad habits by watching and imitating the people around them (Akers, 1998). In places like Anambra, street friends do not just teach technical scamming tricks; they also give social support and praise that makes the crime look like a normal business.

When we look at the financial side, the story is not just about greed. While 45.6% wanted to get rich quickly, 39.1% were actually suffering from deep poverty. This means we cannot just say cybercrime is caused by only greed or only hunger. Instead, it is a mix of financial pressures and the high desire for luxury lifestyles. This view is supported by top researchers like Obianagwa et al. (2023), Uchime et al. (2024), and Willie et al. (2022), who all noted that high youth unemployment and lack of good job opportunities push many Nigerian youths into internet fraud.

The fact that 66.4% of the inmates believed they would never get caught is a major lesson. According to Rational Choice Theory, a criminal will calculate the money he will gain against the risk of going to prison (Cornish & Clarke, 1986). If the money is sweet and the security looks weak, they will take the jump. This tells us that to stop cybercrime, cybersecurity policies must not just block fraud links, but they must make arrests and punishments highly visible so that youths will know that the law is real.

Finally, the fact that only 46.7% had advanced IT skills proves that more than half of the fraudsters inside the cells are not computer geniuses. This supports the warnings by Bada and Nurse (2021) and Edwards et al. (2022) that we should stop treating all cybercriminals as equal tech gurus. Prison authorities in Anambra State must test every inmate to find out if they are real software hackers or just smooth-talking social engineers, so they can give them the right rehabilitation counseling.

Table 4: Cybersecurity, Criminal Profiling and Rehabilitation Outcomes

Indicator	Yes (%)	No (%)	Not sure / Undecided (%)
Aware of law-enforcement profiling	61.2%	38.8%	–
Profiling contributed to arrest	57.6%	24.4%	18.0%
Perception of cybercrime changed during incarceration	69.5%	30.5%	–
Profiling and cybersecurity improve rehabilitation	73.4%	11.3%	15.3%
Intend to redirect digital skills to legitimate work	64.8%	19.4%	15.8%

Source: Field Survey, 2026.

The facts in Table 4 show that 61.2% of the inmates already knew that security agents use digital profiling to fish out internet fraudsters, and 57.6% believed that this profiling method was what led to their own arrest. More importantly, a large majority (69.5%) admitted that their bad mindset about cybercrime has completely changed since they entered prison. Also, 73.4% agreed that combining criminal profiling with prison cybersecurity can make rehabilitation much better, while 64.8% expressed a strong desire to use their computer skills for clean, legal jobs after they leave prison.

Knowing about digital profiling shows that security agencies are making progress. As Bada and Nurse (2021) explained, understanding the lifestyles, pathways, and habits of fraudsters is the only way to block them successfully. Peersman et al. (2022) also added that when security agencies understand the real motives of financial cybercriminals, they can build better tools to stop them. Our study extends this logic into the prison environment, proving that profiling is not just for catching criminals but also for reforming them inside the cells.

The fact that 69.5% of the inmates changed their thinking inside the prison is good news, but it does not mean that prison lockup automatically fixes bad behavior. True reform depends on the actual counseling programs available and the willingness of the inmate to drop bad habits.

The high number of inmates (64.8%) who want to use their digital skills for good jobs shows that these boys have huge potential. However, since 19.4% said "No" and 15.8% are still undecided, we cannot just assume every tech-savvy inmate will change automatically. As Lim and Thing (2022) noted, effective intervention must cure the initial pressure that drove the youth into crime, while creating real job opportunities for them when they get out. This matches the arguments of Nigerian prison experts who state that rehabilitation can only succeed when there is good staff training and solid support for ex-convicts (Ilori, 2024; Irogbo, 2024; Omoruyi & Ego, 2023).

Table 5: Effectiveness of Existing Cybersecurity Measures in the Correctional Centres

Measure / Outcome	Yes (%)	No (%)	Not sure (%)
Digital restrictions exist (No phones/internet)	88.9%	11.1%	–
Monitoring / surveillance systems exist	72.5%	18.1%	9.4%
Participated in digital / ICT rehabilitation programmes	41.3%	58.7%	–
Measures reduce opportunities for continued cybercrime	54.8%	28.4%	16.8%

Source: Field Survey, 2026.

The data in Table 5 reveals that phone and internet restrictions are very tight, with 88.9% of inmates confirming that they are blocked from using digital devices. Also, 72.5% noted that there are surveillance systems monitoring them. However, a major problem is that only 41.3% of these tech-minded inmates have ever participated in any digital literacy, cybersecurity, or clean ICT training program inside the yard. Even though 54.8% believe these security rules stop them from continuing fraud inside the cells, a total of 45.2% either disagreed or were not sure.

This finding exposes a bad balance between punishment and training. The prison authorities focus heavily on locking up computers and blocking internet signals

(88.9%), but they do very little to train the inmates on how to use their coding and technical minds for legal software jobs (only 41.3%). Real cybersecurity inside a prison should not just be about seizing phones. It should include deep monitoring, smart intelligence, and high staff capacity to handle digital issues.

Furthermore, the fact that nearly half of the inmates (45.2%) doubt the effectiveness of these digital bans shows that simple restrictions do not guarantee perfect security. If the prison guards are not well-trained or if corrupt pathways exist, clever fraudsters can still find ways to connect online.

The extremely low participation in positive ICT training (41.3%) is a huge missed opportunity, especially since these boys are already highly exposed to digital systems. This failure directly mirrors the warnings of Lim and Thing (2022), who argued that anti-cybercrime frameworks must create clear paths for legal rehabilitation. It also agrees with several studies across Nigerian custodial centers which lament that broken rehabilitation structures, lack of computers for training, and poor institutional funding are stopping the Nigerian Correctional Service (NCoS) from performing its real reform duties (Ilori, 2024; Irogbo, 2024; Omoruyi & Ego, 2023).

The final lesson here is that prison cybersecurity in Anambra State must move away from just a total "ban-everything" model. While security restrictions are highly necessary for safety, they must be combined with controlled, well-monitored computer training centers. The goal should be to turn technology from a dangerous crime threat into a powerful rehabilitation tool.

Table 6: Relationship between Cybercrime Typologies, Cybersecurity Efficacy and Criminal Profiling Accuracy

Variables	r-value	p-value	N
Cybercrime typologies and profiling accuracy	.612	< .001	443
Cybersecurity efficacy and profiling accuracy	.584	< .001	443

Source: Field Survey, 2026.

The statistical results in Table 6 show a strong, positive, and highly significant relationship between the types of cybercrime committed and the accuracy of profiling the criminals (\(r = .612, p < .001\)). Because of this strong mathematical evidence, the first null hypothesis was rejected.

This mathematical finding proves that when prison staff have a deep understanding of the specific tricks and patterns of internet fraud, they can easily build accurate profiles for each inmate. This result strongly supports the argument of Bada and Nurse (2021), who stated that cybercriminal profiling must look closely at individual paths and habits instead of just throwing every offender into one general group. Edwards et al. (2022) also showed that cybercriminals have completely different motivations, behaviors, and computer skills, meaning they cannot be treated the same way.

For prison authorities in Anambra State, this means that tracking inmate profiles becomes highly useful only when it captures the exact crime committed, the inmate's IT level, their lifestyle, and their family background. For example, an inmate caught for basic phishing needs a completely different risk profile and rehabilitation guide compared to a high-level hacker who breaches major networks.

The test also revealed another strong and positive relationship between the effectiveness of prison cybersecurity rules and the accuracy of profiling inmates (\(r = .584, p < .001\)). Because of this, the second null hypothesis was also rejected.

This second result shows that when a prison has active and strong cybersecurity tracking systems, it becomes much easier to study and understand the inmates. A clear explanation for this link is that good digital security systems provide clear facts and data about what the inmates are doing online, their access habits, and potential security risks. However, we must not look at this correlation as automatic proof that good cybersecurity causes perfect profiling. Other important institutional factors, such as the level of staff training, data management, and the quality of court risk reports, also influence both sides.

Even with that, this result directly supports the main argument of this thesis: prison digital safety and criminal profiling must never be treated as separate jobs. Strong cybersecurity provides the real-time facts needed to study inmate risks, while accurate profiling helps the Nigerian Correctional Service (NCoS) know the exact level of internet blocking, monitoring, and training to give to each inmate.

4.6 Qualitative Evidence from the Interviews

The direct personal interviews conducted with the 10 selected inmates gave deeper human context to the numbers from the questionnaires. These face-to-face stories focused heavily on why they did it, how friends pushed them, their IT skills, and how they see prison rehabilitation. Interestingly, these personal stories perfectly agreed with the numbers from the general survey.

First, the inmates' real-life stories showed that entering cybercrime is not just about having advanced computer

skills. Instead, a mix of street friendships, heavy economic hunger, seeing easy opportunities, and believing they would never be caught all combined to push them into fraud. This agreement with the questionnaire numbers proves that youth cybercrime is a multi-sided human problem.

Second, the stories from the interviews concerning peer relationships strongly backed up the survey result where 58.5% of the respondents blamed friends. This supports the findings of Orjiakor et al. (2022) and Onwuchekwe et al. (2025), who both proved that social environment and peer groups are the primary pathways where young Nigerians learn and normalize internet scams.

Similarly, the words of the inmates concerning how they viewed police arrests before going to prison matched the survey fact that 66.4% had no fear of arrest. From the view of **Rational Choice Theory**, this zero fear makes fraud look highly attractive because the youths only look at the thousands of dollars they will make while ignoring the weak security systems around them (Cornish & Clarke, 1986).

Finally, the interviews provided heavy backing for prison reform outcomes. The fact that these inmates are highly willing to turn their computer talents toward legal IT jobs shows that their digital skills can be turned from a dangerous threat into a great economic resource for Nigeria. However, the qualitative facts also warn us that we need highly supervised and structured prison programs; we must not just assume that an inmate will change his life automatically without solid institutional help (Lim & Thing, 2022).

5. Discussion And Conclusion

The facts gathered in this study clearly prove that cybercrime among inmates inside Anambra State correctional centers is not a one-way issue. Most of the inmates were locked up for everyday online fraud ("yahoo-yahoo") and phishing scams, while only a few did hardcore computer hacking. This proves that cybercrime in Anambra is mostly about using simple phone tricks, fake profiles, and smooth-talking to cheat people out of money, rather than being a computer genius. At the same time, bad peer groups, the desire to ride big cars and look rich, family financial problems, and the strong belief that security agents would never catch them emerged as the biggest human and economic factors driving these youth.

These results strongly support the main idea of this thesis that criminal profiling must look beyond basic facts like age or gender. As Bada and Nurse (2021) and Edwards et al. (2022) showed, internet fraudsters have completely different computer capabilities, life motives, and pathways into crime. Our current study reinforces this position inside the prison walls by showing that convicted inmates differ heavily. Right now, Nigerian prisons treat every cybercriminal the same way—by just locking them up and treating them generally. But a boy who only used smooth-talk to collect money from an online lover needs a different kind of counseling and supervision compared to a tech-savvy boy who can bypass network securities.

The behavioral discoveries can also be easily understood through the theories used in this paper. First, Social Learning Theory explains why friends and street networks have a massive influence on these youths, especially where scamming methods and mental excuses are shared through everyday interactions (Akers, 1998). This matches what Onwuchekwe et al. (2025) and Orjiakor et al. (2022) found in Nigerian local hubs, where street friends give social support that makes the crime look like a normal business. Second, Rational Choice Theory gives a clear explanation for why the inmates had no fear of arrest; they calculated the sweet rewards against the weak police systems and took the risk (Cornish & Clarke, 1986). Third, Routine Activity Theory highlights how the availability of easy targets online and the lack of strong internet monitoring setups create the perfect environment for these crimes to happen (Cohen & Felson, 1979).

Looking at the socioeconomic facts, financial problems and the hunger for luxury items are highly important, but they should not be treated as the only reasons for cybercrime. Instead, the evidence shows a deep connection between general economic hardship, individual greed, and available online loopholes. This view perfectly matches existing Nigerian research which links youth cybercrime directly to high unemployment and bad social conditions (Obianagwa et al., 2023; Uchime et al., 2024; Willie et al., 2022).

The biggest problem found in this research is that Nigerian prisons focus only on punishment and blocking devices, while doing almost nothing to reform the inmates. Over 88% of the inmates confirmed that phones and internet are strictly banned inside the yard, but less than half ever got any useful computer training or cybersecurity lessons. Seizing their phones without teaching them a better trade will not solve the problem. This is a huge missed opportunity because more than 64% of these boys openly confessed that they are ready to drop "yahoo-yahoo" and use their computer skills for clean IT jobs if they get the chance. Turning their digital minds away from crime and guiding them into legal IT work is the only permanent way to reduce crime.

Therefore, this study concludes that fixing cybercrime in Anambra State correctional centers requires a realistic approach that combines strict discipline with real handwork. The Nigerian Correctional Service (NCoS) must move past just locking boys in cells and banning phones. They need to set up monitored computer rooms where these

boys can learn legal programming, coding, or web design. They also need to provide strong counseling to wash away the "get-rich-quick" mindset, and help them find small businesses or jobs when they leave the prison, which aligns with recent correctional studies (Ilori, 2024; Irogbo, 2024; Omoruyi & Ego, 2023). In the final analysis, we cannot calculate the success of prison security by how many phones the wardens seized this month. The true test of success is whether these boys will go back to internet fraud or become useful citizens after they open the prison gates.

6. Recommendations

Based on the study findings, the following recommendations were proposed:

1. **Stop the "One-Size-Fits-All" Treatment:** The Nigerian Correctional Service (NCoS) in Anambra State must stop treating every internet fraudster the same way. When new inmates arrive, wardens should test their actual skills to separate smooth-talking romance scammers from highly technical hackers. This will help the prison give each inmate the exact type of counseling and monitoring he needs.
2. **Move from Seizing Phones to Monitored Training:** Simply banning phones (88.9%) and locking inmates in cells will not cure cybercrime. The prison authorities should partner with tech companies or government bodies like NITDA to set up highly monitored computer rooms. In these rooms, inmates who are willing to change (64.8%) can learn clean programming, web design, and legal cybersecurity. This turns their digital brains away from crime into a useful resource.
3. **Provide Anti-Greed Psychological Counseling:** Since peer pressure (58.5%) and the mad hunger to look rich (45.6%) are major drivers, the prison must invite religious leaders, psychologists, and reformed ex-fraudsters to give heavy orientation talks. These sessions must specifically target and wash away the "get-rich-quick" mindset, teaching the inmates the value of honest labor.
4. **Train Prison Guards on Modern Cyber-Awareness:** To block the underground channels through which inmates secretly get phones inside the yards, prison staff need better training. Wardens should be trained on digital surveillance and modern tricks used by fraudsters so they can catch security leaks early.
5. **Create Post-Release Jobs and Small Business Support:** Since poverty (39.1%) and high youth unemployment push these inmates into fraud, rehabilitation should not end at the prison gate. The Anambra State government should create a pathway where reformed tech-inmates can access small business grants, programming internships, or clean IT jobs immediately after release. If they have a legal way to make money, they will not return to "yahoo-yahoo".

7. References

1. Adewopo, VA, Azumah, SW, Yakubu, MA, Gyamfi, EK, Ozer, M., & Elsayed, N. (2025). Comprehensive analytical review of cybercrime and cyber policy in West Africa. *Journal of Electrical Systems and Information Technology* , *12* , Article 20. https://doi.org/10.1186/s43067-025-00216-x
2. Akers, RL (1998). *Social learning and social structure: A general theory of crime and deviance* . Northeastern University Press.
3. Bada, M., & Nurse, JRC (2021). Profiling the cybercriminal: A systematic review of research. *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* , 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478246
4. Campobasso, M., Rădulescu, R., Brons, SHJP, & Allodi, L. (2023). *You can tell a cybercriminal by the company they keep: A framework to infer the relevance of underground communities to the threat landscape* . arXiv. https://arxiv.org/abs/2306.05898
5. Cohen, LE, & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* , *44* (4), 588–608. https://doi.org/10.2307/2094589
6. Cornish, DB, & Clarke, RVG (Eds.). (1986). *The reasoning criminal: Rational choice perspectives on offending* . Springer-Verlag.
7. Edwards, M., Williams, E., Peersman, C., & Rashid, A. (2022). *Characterizing cybercriminals: A review* . arXiv. https://arxiv.org/abs/2202.07419
8. European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024* . https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
9. Europol. (2024). *Internet organized crime threat assessment (IOCTA) 2024* . Publications Office of the European Union. https://doi.org/10.2813/442713
10. Ilori, OM (2024). Correctional institution (prison) and the control of recidivism among ex-convicts in Southwest Nigeria. *The Malaysian Journal of*

Social Administration , *18* , 49–69. https://doi.org/10.22452/18sp/49.69

11. International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). https://www.itu.int/pub/D-HDB-GCI.01-2024

12. INTERPOL. (2024). *African cyberthreat assessment report 2024* . https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

13. Irogbo, PU (2024). The imperatives of inmates' rehabilitation programs: A study of Delta State correctional centers. *International Journal of Intellectual Discourse* , *7* (2), 327–337. https://ijidjournal.org/index.php/ijid/article/view/571

14. Lim, JWZ, & Thing, VLL (2022). *Towards effective cybercrime intervention* . arXiv. https://arxiv.org/abs/2211.09524

15. National Bureau of Statistics. (2024). *Nigeria labor force survey Q1 2024* . https://www.nigerianstat.gov.ng/elibrary/read/1241562

16. Obianagwa, CE, Ngoka, RO, Uwaechia, OG, Ezugwu, IH, Okpala, JC, & Ayadiuno, RU (2023). Youth unemployment and cybercrime in Nigeria. *African Renaissance* , *20* (2), 145–168. https://doi.org/10.31920/2516-5305/2023/20n2a9

17. Okeke, N., & Onyekachukwu, IO (2024). Cybercrime and digital fraud among university students in Lagos, Nigeria: Socio-economic drivers and prevention approaches. *Journal of Research in Social Science and Humanities* , *3* (9), 13–21. https://doi.org/10.56397/JRSSH.2024.09.02

18. Omoruyi, OL, & Ego, CP (2023). From prison to society: The burden of inmates' rehabilitation, reintegration and recidivism in Nigeria custodial centers. *Journal of Social Theory and Research*, *3* (2), 88–104. https://publications.jostar.org.ng/prison-society-burden-inmates-rehabilitation-reintegration-and-recidivism-nigeria-custodial-centres

19. Onwuchekwe, SI, Onyeoziri, V., Ibekwe, CC, Madu, TE, Nweke, GI, & Agbodike, M. (2025). Influence of peer pressure on youth involvement in cybercrime in Onitsha North Local Government Area of Anambra State, Nigeria. *International Journal of Research* , *12* (11), 107–134. https://doi.org/10.5281/zenodo.17565497

20. Onyeachu, CK, Okoro, IC, & Ugwuoke, MM (2025). The impact of cyber-crime and violent extremism on socio-economic development in Nigeria. *Discover Global Society* , *3* , Article 72. https://doi.org/10.1007/s44282-025-00195-4

21. Orjiakor, CT, Ndiwe, CG, Anwanabasi, P., & Onyekachi, BN (2022). How do internet fraudsters think? A qualitative examination of pro-criminal attitudes and cognitions among internet fraudsters in Nigeria. *The Journal of Forensic Psychiatry & Psychology* , *33* (3), 428–444. https://doi.org/10.1080/14789949.2022.2051583

22. Palmieri, M., Shortland, N., & McGarry, PL (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior* , *120* , Article 106745. https://doi.org/10.1016/j.chb.2021.106745

23. Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals* . arXiv. https://doi.org/10.48550/arXiv.2203.08642

24. Petherick, W., & Brooks, N. (2020). Reframing criminal profiling: A guide for integrated practice. *Psychiatry, Psychology and Law* , *28* (5), 694–710. https://doi.org/10.1080/13218719.2020.1837030

25. Portela, M., Castillo, C., Tolan, S., Karimi-Haghighi, M., & Pueyo, AA (2024). A comparative user study of human predictions in algorithm-supported recidivism risk assessment. *Artificial Intelligence and Law* , *33* , 471–517. https://doi.org/10.1007/s10506-024-09393-y

26. Sani, KM, Hassan, MA, Danjuma, AH, Adam, MM, Nadama, SG, Udu, MS, & Mohammed, F. (2024). Study on cybercrime awareness among youths in Kaduna South Local Government Area, Kaduna State, Nigeria. *International Journal of Indian Psychology*, *12* (4), 47–57. https://doi.org/10.25215/1204.006

27. Uchime, VO, Molokwu, UC, & Ewa, OO (2024). War against cybercrime: Assessing the role of Nigerian governments in the promotion of cybercrime among Nigerian youths, 2000-2020. *EBSU Journal of Social Sciences and Humanities* , *14* (4), 112–130. https://www.ebsu-jssh.com/index.php/EBSUJSSH/article/view/193

28. Willie, CE, Mboho, KS, & Oyosoro, FI (2022). Unemployment, ritual killings: A new dimension of cyber criminality among Nigerian youths. *Research Journal of Humanities and Cultural Studies*, *1* (1), 31–40.

https://www.embarpublishers.com/assets/articles/1651183945.pdf

29. World Bank. (2024). *Nigeria development update: Staying the course on reforms: Progress amid pressing challenges*. World Bank Group. https://www.worldbank.org/en/news/press-release/2024/10/17/nigeria-staying-the-course-on-reforms-progress-amidst-challenges

30. World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/