*FUDMA Journal of Sciences (FJS)*
*ISSN online: 2616-1370*
*ISSN print: 2645 - 2944*
*Vol. 10 No. 9, May, 2026, pp 31 – 40*
*DOI:* https://doi.org/10.33003/fjs-2026-1009-4561

# The Relationship Between Internet Fraud and Psychoactive Substance Use Disorder: A Narrative Review

**[1]Joshua Falade, [2]Oluwafemi Blessing Ajiboye, [3]Benjamin Adekunle Eegunranti, *[4]Foluso Olamide Ojo**

[1]Mental Health Department, University of Medical Sciences, Ondo, Nigeria
[2]Mental Health Department, Ladoke Akintola University of Technology, Ogbomoso,Nigeria
[3]Department of Psychiatry, Ladoke Akintola University of Technology, Ogbomoso, Nigeria
[4]Departemnt of Anatomy, University of Ilesa, Ilesa, Nigeria

*Corresponding authors' email: foluso_ojo@unilesa.edu.ng Phone: +2347062328364

**Received:** 04 May 2026
**Accepted:** 08 May 2026
**Published:** 16 June 2026

**ABSTRACT**

Increase in internet fraud is a growing public health issue, particularly in relation to substance use disorders among youth and adolescents. Review explores the complex relationship between internet fraud and drug addiction, focusing on potential solutions to reduce addiction, particularly in young people. A comprehensive search was conducted between March and November 2023 across Google Scholar, PubMed, and the Cochrane Library to gather articles on internet fraud and drug addiction. The internet serves various roles, including cybercrime such as identity theft, online drug trafficking, and cyberstalking, which introduce unique risks. Addiction is influenced by neurobiological, psychological, and societal factors, with the brain's reward system, genetics, environment, and peer pressure playing key roles. The relationship between internet fraud and addiction is bidirectional, where each worsens the other. The review emphasizes the need to raise awareness about the interconnected risks of internet fraud and drug abuse, particularly for youth.

**Keywords:** Internet fraud, Drug addiction, Relationship, Cyberstalking, substance use

## INTRODUCTION

The global computer network, known as the internet, links billions of computers worldwide. Its official commencement took place on January 1, 1983, serving as a platform for government researchers to exchange information. Presently, there are 3.20 billion internet users worldwide, with noteworthy expansion observed in developing economies (Haldar et al., 2023). Services offered on the internet encompass various communication tools like Voice over Internet Protocol (VoIP), video conferencing, email, and instant messaging. File transfer services utilize protocols such as File Transfer Protocol (FTP) to facilitate the sharing of documents and data. Additionally, directory services like Domain Name System (DNS) and Lightweight Directory Access Protocol (LDAP) play a crucial role in mapping network resource names to addresses and offering cross-platform authentication (Hughes, 2022). Electronic commerce (E-commerce) allows customers to purchase products and services online, and it has evolved significantly since its inception. Network management services like ping and traceroute help internet (IT) administrators to monitor and resolve network-related issues. Time services synchronize computer clocks with standards like Greenwich Mean Time (GMT) or Coordinated Universal time (UTC) using network time protocol (NTP). Search engine services enable users to find web pages based on search queries, with results ranked by relevance. Some search engines accept payments from commercial entities to prioritize their websites in search results, which is labeled as advertising (Erdmann et al., 2022).

Fraud is not a new phenomenon because it has always been around since human history. Its definition and outcomes on victims have not changed (Korsell, 2020). With the use of the Internet for commercial purpose, the method of perpetration of fraudulent activities has evolved to include online capabilities. In other words; the Internet has opened up a door for the development of a new criminal sector of fraud (Rossy and Ribaux, 2020). The scary aspect of this type of new fraud is that perpetrators can now use the anonymous advantage of the Internet to cause harm (Davis and Arrigo, 2021). Since the Internet works on real time, a prospective victim can be harmed much more easily and quickly. It is even possible for the criminal to harm the same victim again and again because the fraudulent electronic transactions can be repeatedly processed within a short period of time (Purnomo and Hartanto, 2023).

A drug is any substance that affects the structure or function of a living organism (Pernice and Scott, 2022) while Addiction is defined as a state of dependence produced either by the habitual taking of drugs or by regularly engaging in certain behavior (Lüscher et al., 2020). The prevalence of drug addiction can change over time and can vary significantly between different regions and communities. Monitoring trends and implementing evidence-based prevention and intervention programs are key strategies in addressing this public health issue (Robinson et al., 2019). Encouraging open communication between parents, educators, and adolescents about the risks of substance use and addiction is important in reducing the prevalence of drug addiction among this age group (Nawi et al., 2021)

A strong link exists between internet fraud and drug addiction, with many individuals turning to internet fraud to finance their drug habits. The allure of quick and easy money can be particularly enticing for those grappling with substance abuse issues (Irwin-Rogers, 2019). Furthermore, drug use can impair one's judgment and decision-making abilities, rendering them more vulnerable to engaging in fraudulent activities. Conversely, falling victim to internet fraud can also lead individuals down the path of drug addiction as a coping mechanism (Irwin-Rogers, 2019). The emotional turmoil resulting from scams or significant financial losses may drive people to resort to substance abuse as a means of seeking

solace or self-medication. The undeniable connection between internet fraud and drug addiction necessitates comprehensive strategies that emphasize prevention through education and awareness programs (Chen and Wawrzynski, 2021). Simultaneously, it is vital to offer support and treatment options for individuals affected by both challenges concurrently.

The aim of the narrative review is to discuss the interplay between internet fraud and psychoactive substance use disorders in order to provide possible solution to the menace of psychoactive substance use especially among adolescents and young adult.

**Methodology**

A comprehensive search for articles related to internet fraud, drug addiction, and their correlation was conducted between March and November 2023. Google Scholar, PubMed, and the Cochrane Library were extensively queried

**Historical Evolution of Fraud**

Throughout history, fraud has maintained a long-standing presence, its roots stretching back to ancient and pre-modern civilizations (Kroeze et al., 2021). In ancient Rome, for instance, individuals practiced the art of counterfeiting coins and documents, among other deceptive activities. Pre-modern eras were rife with practices such as forgery, counterfeit currency, and confidence schemes, often preying on individuals and small communities.

The 19th and early 20th centuries witnessed the evolution of fraud as industrialization and urbanization gained momentum. Frauds such as land swindles, snake oil sales, and Ponzi schemes became prevalent (McTominey, 2024). The expansion of mail and telegraph systems gave rise to mail fraud and wire fraud. In the mid-20th century, telemarketing fraud and pyramid schemes took hold, exploiting individuals over telephone lines and coaxing them into parting with their money. Credit card fraud also emerged as a notable concern with the widespread use of credit cards and card payment systems. The late 20th century and early 21st century brought about the advent of the internet and digital technologies, ushering in a new era of online fraud. This included activities like phishing, identity theft, cyber extortion, hacking, online fraud, computer viruses, DoS (Denial-of-Service) attacks, supply chain attacks, botnets, and financial crimes. Notable financial fraud cases, such as the Bernie Madoff Ponzi scheme, served as stark reminders of financial fraud's resilience in contemporary times. Concurrently, insurance fraud, healthcare fraud, and mortgage fraud grew in complexity and frequency (Kroeze et al., 2021). In the mid-21st century, fraud has continued its evolution alongside rapid technological advancements. Online scams have become increasingly sophisticated, and cyber-attacks are now directed at individuals, businesses, and even governments. The surge in mobile payments has given rise to mobile payment fraud, and digital currency-related scams have proliferated (Khder, 2021). Fraudsters have also embraced social engineering techniques like pretexting and baiting as common tactics.

As technology continues to advance, so does the landscape of fraud. Emerging trends include cryptocurrency fraud, deep fake scams, and AI-driven social engineering attacks. Fraud has transcended borders, becoming a global issue, with scams originating from anywhere in the world and targeting victims on a global scale. Efforts to combat fraud have adapted to these changes, with the development of advanced security systems and regulatory measures.

It is vital to recognize that the prevalence and characteristics of fraud can vary significantly from one region to another, influenced by legal systems, socio-economic conditions, and technological infrastructure. As fraud evolves, so too must the strategies for detecting, preventing, and prosecuting fraudulent activities. Public awareness, education, and vigilance remain essential in the ongoing battle against fraud in the modern age

**Types of Internet Fraud**

The internet has proven highly beneficial in numerous ways. Its usage can be broadly categorized into non-commercial and commercial applications (Khder, 2021). The non-commercial facet of the internet encompasses activities not primarily driven by commercial advantage or monetary gain. These include using the internet for educational purposes, communication, entertainment, and information access. In contrast, the commercial aspect is focused on profit generation and can be further divided into legal and illegal realms. Legal commercial internet use involves activities like online product and service sales, digital marketing, online banking, and telecommuting. On the other hand, illegal commercial internet use falls under the realm of cybercrime (Deora, 2021). Cybercrime can be defined as the illicit use of communication devices to commit or facilitate unlawful activities. It involves acts that exploit or target computers or computer networks with the intent to cause harm. Cybercrimes are executed through the use of technology and networked systems, with targets ranging from individuals to business entities and even governmental organizations (Deora et al., 2021). Investigators employ various methods to examine devices suspected of being involved in or targeted by cybercrime. A cybercriminal is an individual or group that utilizes their technological skills to engage in malicious and unlawful activities categorized as cybercrimes. These actors can function independently or as part of a team and often operate within the "Dark Web," where illegal services and products are frequently exchanged (Kaur, and Randhawa, 2020). Cybercriminals encompass a wide range of individuals engaged in activities such as trading illegal online content, perpetrating scams, or even dealing in illegal substances. Some common examples of cybercriminals include black hat hackers, cyberstalkers, cyber terrorists, and scammers (Jaiswal, 2019). Black hat hackers are individuals or groups that partake in unauthorized or malicious activities related to computer systems, networks, and data. Their objectives typically involve breaching security measures, exploiting vulnerabilities, and engaging in illegal activities for personal gain, financial profit, or to cause harm. The extent of their presence in the digital landscape remains largely unknown (Gandhi et al., 2022)

The forms of internet fraud include, Cyber stalking, Cyber terrorism, Hacking, Harvesting, Framing, Meta Tags and Trademark Infringements, Hypertext Links and Deep Linking, Identity Theft, Ransomware Attack, Online Drug Trafficking, Electronic Money Laundering, and Cyber Extortion (Deora and Chudasama, 2021)

***Cyber Stalking***

Cyber stalking involves the use of the Internet or electronic means to trail or harass individuals, groups, or organizations. It encompasses activities such as false accusations, defamation, slander, libel, monitoring, identity theft, threats, vandalism, and solicitation for sex, doxing, and blackmail.(Chang, 2020) Often, cyber stalking is accompanied by real-time or offline stalking, and in many jurisdictions, like California, both are considered criminal offenses. Both types of stalking are driven by a desire to control, intimidate, or exert influence over the victim, and a stalker can be an online stranger or someone known to the

target. They may operate anonymously and even involve others who are unaware of the target's identity (Cohen-Almagor and Trottier, 2020).

Cyber stalking constitutes a criminal offense under state anti-stalking, slander, and harassment laws (Chahal, 2019). Convictions can result in restraining orders, probation, or criminal penalties, including imprisonment. A study by the Bureau of Justice Statistics in the United States found that one in four stalking victims had experienced cyber stalking. Perpetrators used internet-based services like email, instant messaging, global positioning system (GPS), or spyware. The report estimated that around 1.2 million victims had been stalked using technology (Morgan and Truman, 2022). Additionally, the Rape, Abuse and Incest National Network (RAINN) reported that there are approximately 3.4 million stalking victims each year in the United States, with one in four of them reporting cyberstalking experiences (Centers for Disease Control and Prevention, 2025).

***Cyber Terrorism***

Cyber terrorism can be defined as the deliberate use of computers, networks, and the public internet to cause destruction and harm for personal objectives. Highly skilled cyberterrorists can inflict significant damage on government systems, leaving a nation in fear of further attacks. The motivations behind cyberterrorism may be political or ideological, and it can be considered a form of terror (Ali et al., 2022). Cyber terrorism is the premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets (Veerasamy, 2020). There has been some level of confusion in cyber terrorism and information warfare, but the practical difference between these two terms is that cyber terrorism is about causing fear and harm to anyone in the vicinity (bystanders), while information warfare is having a defined target in a war (ideological or declared). Along with these terms there is a phenomenon of cybercrime used frequently by law enforcement agencies. Cyber-crime is a crime committed through the use of information technology (Libicki, 2020). We must point out that the physical forms of cyber terrorism, information warfare, and cybercrime often look very much alike (Libicki, 2020).

***Hacking***

Hacking encompasses the use of computer skills to breach computer systems or websites, often with the intention of causing harm or stealing data (Goni et al., 2022). The definition of hacking varies, ranging from pushing the boundaries of what's possible to employing technology for inventive purposes (Brooks, 2022). These definitions originate from experts like Richard M. Stallman, Eric S. Raymond, Kevin Mitnick, among others, showcasing a diverse range of perspectives, both positive and negative (Mandel, 2021).

The evolution of hacking has occurred through different generations: In the early generations (Pre-Internet): Hacking was primarily driven by curiosity and a thirst for exploration, marked by a lack of organization and a focus on personal knowledge and bragging rights while in the late 20th Century, the growth of the internet ushered in a more malicious form of hacking, with the proliferation of viruses and worms (Felix et al., 2023).

In addition: Hacking took on a more profit-oriented nature, targeting individuals, businesses, and institutions for financial gain in the early 21st Century Hacktivist groups such as Anonymous also emerged (Pei et al., 2022) while in the mid-21st Century (2010s and beyond), hacking has become more frequent and sophisticated, encompassing state-sponsored hacking, cyber espionage, and the rise of ransomware attacks (Dwan et al., 2022). Generational shifts in hacking are evident, with younger generations becoming more involved. Ethical hacking, often known as white hat hacking, gained prominence, backed by formal training and certifications like Certified Ethical Hacker (CEH) (Del-Real and Rodriguez Mesa, 2023)

Laws against hacking differ across the globe, with measures such as the U.S. Computer Fraud and Abuse Act, the UK's Computer Misuse Act, and the European Union's General Data Protection Regulation (Kosseff, 2020). Nigeria has its own laws, including the Cybercrimes Act and the Nigerian Communications Act, to combat (GPS) hacking. The Nigerian Constitution also plays a role in safeguarding citizens' rights in hacking cases (Olusola et al., 2013).

***Harvesting***

Harvesting in the context of fraud involves the deceptive collection of personal or confidential information for malicious purposes, such as identity theft, phishing, spam, or other illicit activities (Alkhalil et al., 2021). There are two main forms of harvesting, firstly, email Harvesting which involves collecting email addresses without the owner's consent, often for sending spam, phishing emails, or cyberattacks and secondly credential Harvesting: which entails fraudulently acquiring login credentials, like usernames and passwords, through various means, including phishing, social engineering, or malicious software, for unauthorized access to online accounts or systems(Peng et al., 2019). There is limited direct empirical research on the specific link between internet harvesting and substance abuse. However, some studies have explored how online platforms, social media, and web content can influence behaviors, including substance abuse.

***Framing and its Role in Internet Fraud***

Framing is a web design technique that divides a website into real-time “frames,” allowing the website owner’s content to appear alongside third-party material within the same window. This can lead to breaches of copyright law (Reurink, 2019). In the context of internet fraud, framing refers to creating a misleading context that deceives users into thinking they are interacting with a legitimate entity when they are not (Angela, 2020). Fraudsters use framing to create fake websites or emails that resemble trusted brands, financial institutions, or other reputable organizations, luring victims into providing personal data like login credentials or credit card numbers (Okpa et al., 2023). It can be part of a broader social engineering strategy, where fraudsters manipulate victims into taking actions like transferring money or clicking on malicious links (Salahdine and Kaabouch, 2019; Wilson et al., 2024). To protect against framing, individuals should verify the legitimacy of websites and communications and follow good cybersecurity practices.

***Meta Tags and Trademark Infringement***

Meta tags are hidden HTML elements within a website’s code that provide information to search engines and users. These tags are crucial for search engine optimization (SEO) but can also lead to trademark infringement if a competitor’s trademark is used inappropriately within the meta tags to deceive users or divert traffic (Nath, 2022). Trademark infringement occurs when a party uses a trademark in a manner that confuses consumers, often diluting the brand's

distinctiveness (Bone, 2019). The unauthorized use of trademarked terms in meta tags can lead to legal action to protect the brand owner's rights (Cicero, 2020; Mahingoda, 2024).

***Hyperlinks, Deep Linking, and Legal Issues***

Hyperlinks, or "links," are elements that enable users to navigate between websites or web pages (Atzenbeck and Nürnberg, 2019; Vu et al., 2021). Deep linking refers to linking directly to a specific page within a website, bypassing the homepage (Szwajdler, 2022). While deep linking provides convenience, it may raise legal and ethical concerns, especially when it bypasses revenue-generating pages or the site's intended navigation structure (Ma et al., 2020). In some cases, such practices have led to legal disputes over intellectual property rights, such as when Playboy™ sued a porn site for using its logo as a link (Barlow, 2021).

***Identity Theft***

Identity theft occurs when cybercriminals steal personal information such as credit card numbers or Social Security numbers to commit fraud or crimes (Zou et al., 2020). It is a serious form of cybercrime where an individual's sensitive data is used for financial gain or other malicious purposes. Thieves may acquire this information through hacking, social engineering tactics like phishing, or stealing physical documents (Burnes et al., 2020).

***Ransomware Attacks***

Ransomware is a type of malware that encrypts a victim's files, rendering them inaccessible, and demands a ransom, often in cryptocurrency, for decryption (Humayun et al., 2021). This attack typically occurs through malicious email attachments or exploiting vulnerabilities in software (O'Kane et al., 2018; Niu, 2022). Once encrypted, the attacker demands payment and provides a decryption key upon receiving the ransom, usually within a specified time frame.

***Online Drug Trafficking***

The rise of cryptocurrency has facilitated the growth of online drug trafficking by enabling anonymous transactions (Martin and Graffman, 2023). This illicit trade, often conducted on the dark web, involves the sale of illegal substances, including narcotics and prescription drugs, without attracting law enforcement attention (Kamphausen and Werse, 2019).

***Electronic Money Laundering***

Electronic money laundering, or transaction laundering, involves disguising illegally obtained funds through electronic means like digital transactions, online banking, or cryptocurrencies (Anika, 2019). Cryptocurrencies are particularly vulnerable to misuse in money laundering due to their pseudonymous nature and ease of online transactions (Anika, 2019). To combat this, governments have begun regulating cryptocurrency exchanges to curb illicit activities (Dupuis and Gleason, 2020).

**Theory of Addiction**

***Biological Theory of Addiction***

The neurobiology of addiction explores the intricate mechanisms behind addiction, from molecular processes to brain functions, focusing on how neurons communicate electrochemically. Understanding neurotransmitters is critical to grasping addiction's origins (Gkintoni, 2021). Addiction is a complex issue affecting millions worldwide, not only through substance abuse but also through behavioral addictions like gambling, gaming, and compulsive eating (Orum et al., 2018). Addiction has three key components: biological, psychological, and societal (Shafiee et al., 2019)

Addiction often begins with the brain's reward system. Substances or behaviors that trigger dopamine release can lead to addiction. Repeated exposure to these stimuli can desensitize the reward system, requiring more of the substance or behavior to achieve the same pleasurable effect (Volkow et al., 2019). At the core of addiction is the brain's reward system, which involves the release of dopamine in key brain regions, such as the nucleus accumbens. This neurotransmitter plays a critical role in reinforcing behaviors and signaling pleasure. The release of dopamine reinforces rewarding behaviors, such as drug use. Over time, repeated drug exposure disrupts the reward system, causing desensitization of dopamine receptors (Bayassi-Jakowicka et al., 2021). This leads to a cycle where more of the substance is needed to achieve the same effect.

Neuroplasticity, the brain's ability to adapt and reorganize, plays a dual role in addiction. On one hand, it allows the brain to adapt to the presence of drugs, making it more resistant to their effects (Bayassi-Jakowicka et al., 2021). On the other hand, this adaptation contributes to cravings and withdrawal symptoms when the drug is no longer available. The brain rewires its reward pathways, prioritizing the pursuit of the drug over other essential activities (Uhl et al., 2021).

The prefrontal cortex (PFC), responsible for decision-making and impulse control, is essential in addiction. Chronic drug use can impair the PFC, reducing the individual's ability to make rational choices and resist cravings. This impaired control contributes to the addiction cycle. Understanding the neurobiology of addiction is crucial for developing effective prevention and treatment strategies (Lees et al., 2021).

The mesolimbic pathway, which involves the release of dopamine in the nucleus accumbens, is central to addiction. This process strengthens the drive to repeat rewarding behaviors, including drug use. However, chronic addiction leads to deregulation of the dopamine system, making the substance or behavior even more compelling (Dresp-Langley, 2023). The Ventral Tegmental Area (VTA), a key component of the brain's reward system, plays a critical role in reinforcing addictive behaviors by associating them with pleasure. Over time, environmental cues linked to addiction can trigger cravings, with the VTA facilitating this association (Volkow et al., 2019).

Addiction also profoundly affects the PFC, impairing cognitive functions like decision-making and impulse control. Chronic substance use weakens the PFC's ability to assess risks and consequences, making impulsive behaviors more likely. Stress and exposure to triggers can further impair PFC control, increasing the risk of relapse (Dresp-Langley, 2023)). Addiction leads to significant structural and functional changes in the brain, contributing to the persistent cycle of addiction. These neuroadaptive changes result in reduced sensitivity to natural rewards and a greater need for the addictive substance (Zhang and Volkow, 2019).

Genetics plays a key role in addiction susceptibility. Certain genetic factors can make individuals more prone to addiction, while environmental influences such as stress or childhood trauma can further increase the risk (Volkow et al., 2019). Addiction is a complex interaction between genetic and environmental factors (Ersche et al., 2020). Although no single gene causes addiction, several genes influence susceptibility by affecting the reward pathway, neurotransmitter systems, and impulse control (Crabbe, 2002). A study in Korea found genetic polymorphisms in adolescents with excessive internet use, linking them to higher harm avoidance and depression scores, highlighting

the genetic basis of behavioral addictions (Kożybska et al., 2022).

***Psychological Theory***

Many individuals with addiction have underlying mental health issues such as depression, anxiety, or trauma (Bayassi-Jakowicka et al., 2021). They may use substances or behaviors as a form of self-medication to alleviate emotional pain. Addiction can also be a way to cope with stress, trauma, or life challenges. The temporary relief or distraction it provides can create a cycle where individuals turn to addictive behaviors to manage difficulties (Volkow et al., 2019). Over time, the brain associates certain cues or environments with the addictive substance or behavior, leading to intense cravings (Antons et al., 2020). This classical conditioning can be a powerful driver of addiction. Understanding the interplay between personality and addiction is important for developing effective prevention and treatment strategies. However, it is essential to note that addiction is a complex phenomenon influenced by a wide range of factors including genetics, environmental influences and social support systems (Volkow et al., 2019). While personality traits can be risk factors, they do not solely determine an individual's likelihood of developing an addiction (Lees et al., 2021).

***Social Theory***

Social influences and peer pressure can contribute to addiction. Acceptance within a particular social group may be tied to engaging in substance use or certain behaviors, making it difficult for individuals to resist. The availability and ease of access to addictive substances or activities, such as alcohol, drugs, or online gambling, can significantly impact addiction rates. Widespread access increases the likelihood of experimentation and addiction. Numerous studies have shown that adolescents and young adults are particularly vulnerable to peer pressure when it comes to drug use initiation. Peers can introduce individuals to drugs, encourage experimentation, and facilitate access (Eddie et al., 2019). Research has consistently indicated that peer pressure is a significant factor in the continued abuse of drugs. Adolescents and adults who have friends or peers who use drugs are more likely to engage in substance abuse themselves (Nawi et al., 2021).

Conformity to social norms plays a crucial role in drug addiction. When individuals perceive drug use as common or socially acceptable within their peer group, they are more likely to use drugs (Kollath-Cattano et al., 2020). Researchers often distinguish between "peer selection" (choosing friends who already use drugs) and "peer influence" (being pressured into drug use by friends). Both can contribute to drug addiction. Some studies have explored the neurobiological mechanisms behind peer pressure and drug addiction. These studies often involve brain imaging to understand how peer influence affects decision-making and reward systems (Kollath-Cattano et al., 2020).

Research also focuses on the development of interventions and prevention strategies that target peer pressure as a risk factor for drug addiction. These can include school-based programs, family interventions, and community initiatives (Nawi et al., 2021). Long-term studies tracking individuals over time have been important in establishing the relationship between peer pressure and drug addiction (McGloin and Thomas, 2019). They can help identify the timing of peer influence and its lasting impact. Cultural factors can significantly influence the extent to which peer pressure leads to addiction (Nawi et al., 2021).

It's important to consider other factors that may interact with peer pressure, such as genetics, family dynamics, socioeconomic status, and mental health (Luo, 2020). These can either amplify or mitigate the effects of peer pressure. With the rise of social media and online communities, researchers have begun to explore the influence of online peers in drug addiction. Online peer pressure can be just as powerful as offline pressure. In a study done in the University of Ibadan, Nigeria, it was said that "yahoo-boys' enjoy a status of big boys and are socially recognized among friends. They also see the internet fraud as a social security to escape exposure to anticipated difficulties (Ojedokun and Eraye, 2012).

**Review on Internet Fraud and Drug Addiction**

Only a few related studies have been carried out to assess fraudulent internet use and drug addiction. Most of the literature focused more on internet addiction rather than drug addiction and internet fraud. Moreover, internet fraud and internet addiction go hand in hand. The scale of health implications of psychoactive substance use, and the number of related deaths, is a growing concern (Peacock et al., 2019). The prevalence of internet fraud among individuals abusing psychoactive substances can vary based on multiple factors, including the type of circumstance, individual circumstances, and the availability of the internet. There is no single statistic that accurately reflects the prevalence of internet fraud in this specific population.

**Contributing Factors to the use of Psychoactive Substances among Individuals Engaged in Internet Fraud**

There is not a direct connection between engaging in internet fraud and substance abuse that applies universally. However, individuals involved in illegal activities, including fraud, may have a variety of personal reasons for substance abuse. These could include stress and pressure, financial mtivation, per ifluence, ecapism, and pychological fctors

***Stress and Pressure***

Engaging in illegal activities, including internet fraud, can be stressful and mentally taxing. Some individuals may turn to drugs as a coping mechanism. Internet fraudsters face numerous stressors due to their constant fear of being caught, constant anxiety, and the pressure to stay ahead of authorities and cyber security measures (McGloin and Thomas, 2019). They also grapple with guilt and internal conflicts between financial gain and moral conscience, leading to feelings of loneliness and depression. The solitary nature of their work isolates them, where trust is scarce, causing feelings of loneliness and depression. A study highlights the multifaceted stressors faced by internet fraudsters in their criminal pursuits, emphasizing the need for social support systems and emotional release. (Kemp and Erades, 2023).

***Peer Influence***

In some cases, involvement in criminal activities may be associated with specific social circles where drug abuse is prevalent. Peer influence can lead individuals to engage in drug abuse (Nawi et al., 2021). Friends or acquaintances who are involved in such activities may pressure or encourage others to join in. When a person's peer group engages in drug abuse, it can normalize the behavior and make it seem socially acceptable. This normalization can lower inhibitions and increase the likelihood of participation. Some individuals engage in addiction to sustain a particular lifestyle or to keep up with their peer group's material possessions (Buil-Gil et al., 2021). Peer influence to maintain this image can drive individuals toward illegal activities. Moreover, young people

who want to fit in and be accepted by their peers may feel compelled to use drugs to gain social approval (Dumbili, 2020). The fear of being rejected or excluded from a peer group can be a powerful motivator (Allen et al., 2022).

***Escapism***

Individuals involved in internet fraud may use drugs as a form of escapism from the reality of their actions or the potential consequences they might face (Kalmár and Kalmár, 2020). People may turn to addiction as a way to escape from their real-life problems, stress, or emotional issues. Past research regards escapism as a negative inducement that leads to adverse consequences when combined with substance use and other addictive activities. Existing knowledge on escapism's connection to addiction is mostly based on studies with restricted populations and lacks a comprehensive view. It can serve as an initial motive, a reinforcer, and an amplifier of addictive behaviors (Jouhki and Oksanen, 2022). Scammers often use manipulation and deception to exploit their victims. This emotional trauma can have a lasting impact on a person's mental health, making them vulnerable to substance abuse as a way to numb or escape their feelings (Taiwo, 2012).

***Psychological Factors***

Some individuals that engaged in illegal activities may have underlying psychological issues that contribute to both their involvement in fraud and substance abuse. Many individuals engage in internet fraud driven by financial motives. This motivation can be influenced by factors such as financial desperation, a desire for material wealth, or a belief that fraudulent activities offer a quick and easy solution to financial problems (Kalmár and Kalmár, 2020). Some individuals engage in fraud by rationalizing their actions, convincing themselves that their fraudulent activities are justified or that they won't cause harm. This cognitive distortion can be influenced by psychological factors, such as moral disengagement or a belief that they are owed something. A lack of empathy for the potential victims of fraud can be a psychological factor that allows individuals to engage in these activities (Monsurat, 2020). A detached or callous attitude toward the impact of their actions can make it easier for them to commit other social vices, including drug abuse.

**Contributing Factors to Internet Fraud among Individuals Engaged in Psychoactive Substance use**

Individuals who are addicted to psychoactive drugs may engage in internet fraud for various reasons, but it is crucial to recognize that not everyone with a substance addiction participates in illegal activities (Nawi et al., 2021). However, for those who do, here are some potential reasons, financial need, impaired judgment, desperation, ecapism, per influence,

***Financial Need***

Drug addiction can be an expensive habit, and individuals may turn to illegal activities like internet fraud to fund their substance use (Ojedokun and Eraye, 2012). There are some groups of theories that explain this factor. The first group of theories includes what are sometimes called 'drug-use-causes-crime' and 'crime-causes-drug-use' explanations. These are both direct versions of the connection in that one of the variables is seen as causing the other. The most common 'drug-use-causes-crime' theory is the 'enslavement theory' or 'economic necessity' theory (Jouhki and Oksanen, 2022). This is the view that serious drug users will be unable to support their habit through legitimate activities and will resort to crime to fund their drug use.

Drug addiction can lead to a cycle of desperation, where individuals resort to illegal activities like fraud to finance their addiction (Akomea-Frimpong and Andoh, 2020; Haasio et al., 2020; Currie and Schwandt, 2021). The high cost of drugs and potential job loss can cause significant financial strain. As addiction progresses, desperation can lead to seeking financial relief through internet fraud (Barnor et al., 2020). Successful fraudulent activities provide temporary relief, but the financial resources acquired are often insufficient to maintain a drug addiction in the long term, perpetuating a cycle of desperation, fraud, and drug use (Iqbal et al., 2019; Corner, 2023).

***Impaired Judgment***

Substance abuse can impair cognitive functions and decision-making, leading individuals to make risky choices, including involvement in fraud (Jouhki and Oksanen, 2022). Similar to patients with orbitofrontal cortex lesions, substance dependent individuals (SDI) show signs of impairments in decision-making, characterized by a tendency to choose the immediate reward at the expense of severe negative future consequences.

The somatic-marker hypothesis proposes that decision-making depends in many important ways on neural substrates that regulate homeostasis, emotion and feeling. According to this model, there should be a link between abnormalities in experiencing emotions in SDI, and their severe impairments in decision-making in real-life. Growing evidence from neuroscientific studies suggests that core aspects of substance addiction may be explained in terms of abnormal emotional guidance of decision-making. Behavioural studies have revealed emotional processing and decision-making deficits in SDI (Volkow et al., 2019).

***Escapism***

Engaging in internet fraud might serve as a way for individuals to temporarily escape the challenges and stresses associated with drug addiction (Jouhki and Oksanen, 2022). Drug addiction often begins as a means to cope with stress, anxiety, or emotional pain. For some, drugs provide a temporary escape from their problems and feelings. Substance abuse can create feelings of euphoria and altered consciousness, offering an escape from the individual's current reality. The desire to experience these sensations can drive addiction. Escapism through drug use can lead to a cycle of addiction, as individuals continually seek relief from negative emotions by using drugs (Kalmár and Kalmár, 2020). This can result in negative consequences, which further intensify the need to escape through drug use.

**CONCLUSION**

The relationship between internet fraud and drug abuse is complex and can vary among individuals. It's not accurate to generalize as unidirectional or bidirectional, as the relationship may be influenced by numerous factors. The bidirectional rlationship between iternet faud and Drug Abuse reinforcing each other has been explored. Individuals with a pre-existing drug abuse issue might turn to internet fraud to fund their addiction. Conversely, engaging in internet fraud can create stress and legal consequences, leading to increased substance abuse as a coping mechanism. The two behaviors may reinforce each other in a cycle where the consequences of one behavior exacerbate the other.

It is essential to recognize that the relationship between internet fraud and drug abuse is highly individualized. Not everyone engaged in internet fraud abuses drugs, and not all individuals with substance abuse issues turn to illegal

activities. Various factors, including personal vulnerabilities, socioeconomic conditions, mental health, and social influences, contribute to these complex relationships. Treatment and intervention strategies should address both the criminal behavior and substance abuse, considering the unique circumstances of each individual.
The commercial internet is a powerful tool that can be used for both good and bad. It is important to be aware of the potential risks of commercial internet use, especially for young people. By taking steps to reduce these risks, we can help to protect young people from the dangers of psychoactive substance use.

## LIMITATION

The major limitation was the dearth of exposure of researchers' in associating commercial internet use with drug addiction. Both drug abuse and internet fraud are sensitive topics, and individuals may be hesitant to disclose their involvement, leading to underreported data. Individuals involved in drug abuse or internet fraud may face stigma, affecting their willingness to participate in research or provide accurate information.

## List of Abbreviations

VoIP - Voice over Internet Protocol,
FTP-File Transfer Protocol,
DNS- Domain Name System,
LDAP- Lightweight Directory Access Protocol,
IT-internet,
GMT- Greenwich Mean Time,
NTP- network time protocol,
GPS- global positioning system,
CEH -Certified Ethical Hacker,
SEO-search engine optimization,
VTA-Ventral Tegmental Area

## Consent for Publication

The authors gave the consent to publish this review

## Conflict of Interest

There is no conflict of interest to be declared.

## REFERENCES

Akomea-Frimpong, I., & Andoh, C. (2020). Understanding and controlling financial fraud in the drug industry. *Journal of Financial Crime*, *27*(2), 337–354. https://doi.org/10.1108/JFC-06-2019-0076

Ali, S., Shah, S. Z. H.,SUBMITTED Qureshi, S. N., & Tanveer, S. (2022). Impact of cyber-terrorism on national security of Pakistan. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *19*(1), 1456–1468.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, Article 563060. https://doi.org/10.3389/fcomp.2021.563060

Allen, K. A., Gray, D. L., Baumeister, R. F., & Leary, M. R. (2022). The need to belong: A deep dive into the origins, implications, and future of a foundational construct. *Educational Psychology Review*, *34*(2), 1133–1156. https://doi.org/10.1007/s10648-021-09633-6

Angela, N. N., Ijeoma, O. B. I., & Guanah, S. J. (2020). Framing of cybercrime (Yahoo-Yahoo business) by The Guardian and Vanguard newspapers. *The Nigerian Journal of Communication*, *17*(1), 41–61.

Anika, I. E. (2019). *New technology for old crimes? The role of cryptocurrencies in circumventing the global anti-money laundering regime and facilitating transnational crime* [Doctoral dissertation, University of British Columbia]. UBC cIRcle. https://open.library.ubc.ca/

Antons, S., Brand, M., & Potenza, M. N. (2020). Neurobiology of cue-reactivity, craving, and inhibitory control in non-substance addictive behaviors. *Journal of the Neurological Sciences*, *415*, Article 116952. https://doi.org/10.1016/j.jns.2020.116952

Atzenbeck, C., & Nürnberg, P. J. (2019). Hypertext as method. In *Proceedings of the 30th ACM Conference on Hypertext and Social Media* (pp. 29–38). ACM. https://doi.org/10.1145/3342220.3343653

Barlow, B. R. (2021). *The fantastical world of Playboy* [Master's thesis, University of Waterloo]. UWSpace. http://hdl.handle.net/10012/17058

Barnor, J. N. B., Boateng, R., Kolog, E. A., & Afful-Dadzie, A. (2020). Rationalizing online romance fraud: In the eyes of the offender. In *AMCIS 2020 Proceedings* (Paper 21). Association for Information Systems. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21

Bayassi-Jakowicka, M., Lietzau, G., Czuba, E., Steliga, A., Waśkow, M., & Kowiański, P. (2021). Neuroplasticity and multilevel system of connections determine the integrative role of nucleus accumbens in the brain reward system. *International Journal of Molecular Sciences*, *22*(18), Article 9806. https://doi.org/10.3390/ijms22189806

Bone, R. G. (2019). Rights and remedies in trademark law: The curious distinction between trademark infringement and unfair competition. *Texas Law Review*, *98*(7), 1187–1232.

Brooks, T. (2022). *The professionalization of the hacker industry* (arXiv:2207.00890). arXiv. https://doi.org/10.48550/arXiv.2207.00890

Buil-Gil, D., Zeng, Y., & Kemp, S. (2021). Offline crime bounces back to pre-COVID levels, cyber stays high: Interrupted time-series analysis in Northern Ireland. *Crime Science*, *10*(1), 1–16. https://doi.org/10.1186/s40163-021-00149-w

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, *17*, Article 101058. https://doi.org/10.1016/j.pmedr.2020.101058

Centers for Disease Control and Prevention. (2025). National Intimate Partner and Sexual Violence Survey: 2023/2024 stalking data brief. https://www.cdc.gov/nisvs/media/pdfs/stalking-brief.pdf

Chahal, R., Kumar, L., Jindal, S., & Rawat, P. (2019). Cyber stalking: Technological form of sexual harassment. *International Journal of Emerging Technologies*, *10*(3), 367–373.

Chang, W. J. (2020). Cyberstalking and law enforcement. *Procedia Computer Science*, *176*, 1188–1194. https://doi.org/10.1016/j.procs.2020.09.114

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, *66*, Article 102655. https://doi.org/10.1016/j.scs.2020.102655

Cicero, T. J., Ellis, M. S., & Kasper, Z. A. (2020). Polysubstance use: A broader understanding of substance use during the opioid crisis. *American Journal of Public Health*, *110*(2), 244–250. https://doi.org/10.2105/AJPH.2019.305412

Cohen-Almagor, R., & Trottier, D. (2022). Internet crime enabling: Stalking and cyberstalking. In K. Arai (Ed.), *Intelligent computing: Proceedings of the 2022 Computing Conference* (pp. 843–859). Springer International Publishing. https://doi.org/10.1007/978-3-031-10461-9_59

Corner, T. (2023). *A mixed methods exploration of the lived experience of pre-addiction and long-term recovery* [Doctoral dissertation, Bournemouth University]. BURO. https://eprints.bournemouth.ac.uk/

Crabbe, J. C. (2002). Genetic contributions to addiction. *Annual Review of Psychology*, *53*(1), 435–462. https://doi.org/10.1146/annurev.psych.53.100901.135142

Currie, J., & Schwandt, H. (2021). The opioid epidemic was not caused by economic distress but by factors that could be more rapidly addressed. *The Annals of the American Academy of Political and Social Science*, *695*(1), 276–291. https://doi.org/10.1177/0002716221997174

Davis, S., & Arrigo, B. (2021). The dark web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime, Law and Social Change*, *76*(4), 367–386. https://doi.org/10.1007/s10611-021-09963-2

Del-Real, C., & Rodriguez Mesa, M. J. (2023). From black to white: The regulation of ethical hacking in Spain. *Information & Communications Technology Law*, *32*(2), 207–239. https://doi.org/10.1080/13600834.2022.2098395

Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of Communication Engineering & Systems*, *11*(1), 1–6.

Dresp-Langley, B. (2023). From reward to anhedonia — Dopamine function in the global mental health context. *Biomedicines*, *11*(9), Article 2469. https://doi.org/10.3390/biomedicines11092469

Dumbili, E. W. (2020). Cannabis normalization among young adults in a Nigerian city. *Journal of Drug Issues*, *50*(3), 286–302. https://doi.org/10.1177/0022042620908096

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *Journal of Financial Crime*, *28*(1), 60–74. https://doi.org/10.1108/JFC-06-2020-0113

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the cyber seas: Are state-sponsored hackers modern-day privateers? *Law, Technology and Humans*, *4*(1), 49–62. https://doi.org/10.5204/lthj.2267

Eddie, D., Hoffman, L., Vilsaint, C., Abry, A., Bergman, B., Hoeppner, B., & Kelly, J. F. (2019). Lived experience in new models of care for substance use disorder: A systematic review of peer recovery support services and recovery coaching. *Frontiers in Psychology*, *10*, Article 1052. https://doi.org/10.3389/fpsyg.2019.01052

Erdmann, A., Arilla, R., & Ponzoa, J. M. (2022). Search engine optimization: The long-term strategy of keyword choice. *Journal of Business Research*, *144*, 650–662. https://doi.org/10.1016/j.jbusres.2022.02.017

Ersche, K. D., Meng, C., Ziauddeen, H., Stochl, J., Williams, G. B., Bullmore, E. T., & Robbins, T. W. (2020). Brain networks underlying vulnerability and resilience to drug addiction. *Proceedings of the National Academy of Sciences*, *117*(26), 15253–15261. https://doi.org/10.1073/pnas.1921037117

Felix, A. O., Olabode, O. J., & Ayeni, J. K. (2023). The criminalization of the internet and cybercrime in general: A comprehensive study. *Scientific and Practical Cyber Security Journal*, *7*(1), 4–14. https://doi.org/10.37486/2664-9055.7.1.2023

Gandhi, F., Pansaniya, D., & Naik, S. (2022). Ethical hacking: Types of hackers, cyber attacks and security. *International Research Journal of Innovations in Engineering and Technology*, *6*(1), 28–33. https://doi.org/10.47001/IRJIET/2022.601007

Gkintoni, E., Meintani, P. M., & Dimakos, I. (2021). Neurocognitive and emotional parameters in learning and educational process. In *ICERI2021 Proceedings* (pp. 2588–2599). IATED. https://doi.org/10.21125/iceri.2021.0635

Goni, O. (2022). Cyber crime and its classification. *International Journal of Electronics Engineering and Applications*, *10*(1), 17–22.

Haasio, A., Harviainen, J. T., & Savolainen, R. (2020). Information needs of drug users on a local dark web marketplace. *Information Processing & Management*, *57*(2), Article 102080. https://doi.org/10.1016/j.ipm.2019.102080

Haldar, A., Sucharita, S., Dash, D. P., Sethi, N., & Padhan, P. C. (2023). The effects of ICT, electricity consumption, innovation and renewable power generation on economic growth: An income level analysis for the emerging economies. *Journal of Cleaner Production*, *384*, 135607. https://doi.org/10.1016/j.jclepro.2022.135607

Hughes, L. E. (2022). *Pro active directory certificate services: Creating and managing digital certificates for use in Microsoft networks*. Apress. https://doi.org/10.1007/978-1-4842-7486-6

Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105–117. https://doi.org/10.1016/j.eij.2020.05.003

Iqbal, M. N., Levin, C. J., & Levin, F. R. (2019). Treatment for substance use disorder with co-occurring mental illness.

*FOCUS: The Journal of Lifelong Learning in Psychiatry*, *17*(2), 88–97. https://doi.org/10.1176/appi.focus.20180042

Irwin-Rogers, K. (2019). Illicit drug markets, consumer capitalism and the rise of social media: A toxic trap for young people. *Critical Criminology*, *27*(4), 591–610. https://doi.org/10.1007/s10612-019-09463-9

Jaiswal, M. (2019). Cybercrime categories and prevention. *International Journal of Creative Research Thoughts*, *7*(4), 929–933. https://ijcrt.org/papers/IJCRT1904292.pdf

Jouhki, H., & Oksanen, A. (2022). To get high or to get out? Examining the link between addictive behaviors and escapism. *Substance Use & Misuse*, *57*(2), 202–211. https://doi.org/10.1080/10826084.2021.2002031

Kalmár, G. (2020). Addiction and escapism. In G. Kalmár, *Post-crisis European cinema: White men in off-modern landscapes* (pp. 109–147). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-37665-7_5

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, *73*, 281–287. https://doi.org/10.1016/j.drugpo.2019.07.031

Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications*, *112*(4), 2131–2158. https://doi.org/10.1007/s11277-020-07143-2

Kemp, S., & Erades Pérez, N. (2023). Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health*, *20*(7), Article 5404. https://doi.org/10.3390/ijerph20075404

Khder, M. A. (2021). Web scraping or web crawling: State of art, techniques, approaches and application. *International Journal of Advances in Soft Computing and Its Applications*, *13*(3), 145–168. https://doi.org/10.15849/IJASCA.211128.11

Kollath-Cattano, C., Hatteberg, S. J., & Kooper, A. (2020). Illicit drug use among college students: The role of social norms and risk perceptions. *Addictive Behaviors*, *105*, Article 106289. https://doi.org/10.1016/j.addbeh.2020.106289

Korsell, L. (2020). Fraud in the twenty-first century. *European Journal on Criminal Policy and Research*, *26*(3), 285–291. https://doi.org/10.1007/s10610-020-09461-4

Kosseff, J. (2020). Hacking cybersecurity law. *University of Illinois Law Review*, *2020*(3), 811–856.

Kożybska, M., Kurpisz, J., Radlińska, I., Skwirczyńska, E., Serwin, N., Zabielska, P., & Flaga-Gieruszyńska, K. (2022). Problematic internet use, health behaviors, depression and eating disorders: A cross-sectional study among Polish medical school students. *Annals of General Psychiatry*, *21*(1), Article 5. https://doi.org/10.1186/s12991-022-00381-7

Kroeze, R., Dalmau, P., & Monier, F. (2021). Introduction: Corruption, empire and colonialism in the modern era — Towards a global perspective. In R. Kroeze, P. Dalmau, & F. Monier (Eds.), *Corruption, empire and colonialism in the modern era: A global perspective* (pp. 1–19). Springer Singapore. https://doi.org/10.1007/978-981-33-6452-6_1

Lees, B., Garcia, A. M., Debenham, J., Kirkland, A. E., Bryant, B. E., Mewton, L., & Squeglia, L. M. (2021). Promising vulnerability markers of substance use and misuse: A review of human neurobehavioral studies. *Neuropharmacology*, *187*, Article 108500. https://doi.org/10.1016/j.neuropharm.2021.108500

Libicki, M. C. (2020). The convergence of information warfare. In T. J. Mahnken & J. A. Maiolo (Eds.), *Information warfare in the age of cyber conflict* (pp. 15–26). Routledge. https://doi.org/10.4324/9780429399718-2

Luo, L. (2020). *Principles of neurobiology* (2nd ed.). Garland Science.

Lüscher, C., Robbins, T. W., & Everitt, B. J. (2020). The transition to compulsion in addiction. *Nature Reviews Neuroscience*, *21*(5), 247–263. https://doi.org/10.1038/s41583-020-0281-z

Ma, Y., Hu, Z., Gu, D., Zhou, L., Mei, Q., Huang, G., & Liu, X. (2020). Roaming through the castle tunnels: An empirical analysis of inter-app navigation of Android apps. *ACM Transactions on the Web*, *14*(3), 1–24. https://doi.org/10.1145/3397192

Mahingoda, C. B. (2024). Challenges and frontiers in intellectual property rights amidst the rise of artificial intelligence. *SLIIT Journal of Humanities and Sciences*, *4*(2), 1–15. https://doi.org/10.54389/ABSP3716

Mandel, N. (2021). "To float, to hide, to disappear": The hacker in *The Circle*. *Mosaic: An Interdisciplinary Critical Journal*, *54*(3), 85–101. https://doi.org/10.1353/mos.2021.0019

Martin, J., & Graffman, N. (2023). Drug trafficking on cryptomarkets and the role of organized crime groups. *Forensic Science International: Synergy*, *7*, Article 100326. https://doi.org/10.1016/j.fsisyn.2023.100326

McGloin, J. M., & Thomas, K. J. (2019). Peer influence and delinquency. *Annual Review of Criminology*, *2*(1), 241–264. https://doi.org/10.1146/annurev-criminol-011518-024551

McTominey, A. (2024). Bibliography of urban history 2024. *Urban History*, *51*(4), 915–974. https://doi.org/10.1017/S0963926824000506

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: A study of the Yahoo boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, *14*(1), 300–315. https://doi.org/10.5281/zenodo.4391452

Morgan, R. E., & Truman, J. L. (2022). *Stalking victimization, 2019* (NCJ 304081). U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://bjs.ojp.gov/content/pub/pdf/sv19.pdf

Nath, K. (2022). *Evolution of the internet from web 1.0 to metaverse: The good, the bad and the ugly*. TechRxiv. https://doi.org/10.36227/techrxiv.19742415.v1

Nawi, A. M., Ismail, R., Ibrahim, F., Hassan, M. R., Manaf, M. R. A., Amit, N., & Shafurdin, N. S. (2021). Risk and protective factors of drug abuse among adolescents: A systematic review. *BMC Public Health*, *21*, Article 2088. https://doi.org/10.1186/s12889-021-11906-2

Niu, S., Yu, F., Song, M., Han, S., & Wang, C. (2022). Specified keywords search scheme for EHR sharing. *Soft Computing*, *26*(18), 8949–8960. https://doi.org/10.1007/s00500-022-07246-3

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the Yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2023). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*(2), 350–372. https://doi.org/10.1057/s41284-021-00322-7

Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Cyber crimes and cyber laws in Nigeria. *The International Journal of Engineering and Science*, *2*(4), 19–25.

Orum, M. H., Kustepe, A., Kara, M. Z., Dumlupinar, E., Egilmez, O. B., Ozen, M. E., & Kalenderoglu, A. (2018). Addiction profiles of patients with substance dependency living in Adiyaman province. *Medical Science*, *7*(2), 369–372. https://doi.org/10.5455/medscience.2017.06.8707

Peacock, A., Bruno, R., Gisev, N., Degenhardt, L., Hall, W., Sedefov, R., & Griffiths, P. (2019). New psychoactive substances: Challenges for drug surveillance, control, and public health responses. *The Lancet*, *394*(10209), 1668–1684. https://doi.org/10.1016/S0140-6736(19)32231-7

Pei, J., Li, D., & Cheng, L. (2022). Media portrayal of hackers in *China Daily* and *The New York Times*: A corpus-based critical discourse analysis. *Discourse & Communication*, *16*(5), 598–618. https://doi.org/10.1177/17504813221083155

Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B., & Wang, G. (2019). What happens after you leak your password: Understanding credential sharing on phishing sites. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (pp. 181–192). ACM. https://doi.org/10.1145/3321705.3329818

Pernice, I. G. A., & Scott, B. (2022). Cryptocurrencies and drug trafficking: A primer for Ohio prosecutors and law enforcement agencies. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4292122

Purnomo, V. D., & Hartanto, R. (2023). Transaction fraud buy and sell online through restitution as criminal addition in the Electronic Information and Transaction Law. *Asian Journal of Community Services*, *2*(3), 265–286. https://doi.org/10.55927/ajcs.v2i3.3660

Reurink, A. (2019). Financial fraud: A literature review. In T. Beck, J. Berg, & M. Blix (Eds.), *Contemporary topics in finance: A collection of literature surveys* (pp. 79–115). Wiley. https://doi.org/10.1002/9781119565178.ch4

Robinson, A., Christensen, A., & Bacon, S. (2019). From the CDC: The Prevention for States program — Preventing opioid overdose through evidence-based intervention and innovation. *Journal of Safety Research*, *68*, 231–237. https://doi.org/10.1016/j.jsr.2018.10.010

Rossy, Q., & Ribaux, O. (2020). Orienting the development of crime analysis processes in police organizations covering the digital transformations of fraud mechanisms. *European Journal on Criminal Policy and Research*, *26*(3), 335–356. https://doi.org/10.1007/s10610-020-09460-5

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), Article 89. https://doi.org/10.3390/fi11040089

Shafiee, S. A., Razaghi, E., & Vedadhir, A. A. (2019). Multi-level approach to theories of addiction: A critical review. *Iranian Journal of Psychiatry and Behavioral Sciences*, *13*(2), Article e88881. https://doi.org/10.5812/ijpbs.88881

Szwajdler, P. (2022). Limitations of the freedom of hyperlinking in the fields of copyright law, trademark law and unfair competition law: Is case-by-case approach sufficient? *Computer Law & Security Review*, *45*, Article 105692. https://doi.org/10.1016/j.clsr.2022.105692

Taiwo, R. (2012). Discursive manipulation strategies in virtual scams in global contexts. In K. St.Amant & S. Kelsey (Eds.), *Computer-mediated communication across cultures: International interactions in online environments* (pp. 143–154). IGI Global. https://doi.org/10.4018/978-1-60960-833-0.ch010

Uhl, G. R., Koob, G. F., & Cable, J. (2019). The neurobiology of addiction. *Annals of the New York Academy of Sciences*, *1451*(1), 5–28. https://doi.org/10.1111/nyas.13989

Veerasamy, N. (2020). Cyberterrorism — The spectre that is the convergence of the physical and virtual worlds. In E. Fransen & M. Lehto (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 27–52). Academic Press. https://doi.org/10.1016/B978-0-12-816464-3.00002-4

Volkow, N. D., Michaelides, M., & Baler, R. (2019). The neuroscience of drug reward and addiction. *Physiological Reviews*, *99*(4), 2115–2140. https://doi.org/10.1152/physrev.00014.2018

Vu, K. P. L., Proctor, R. W., & Hung, Y. H. (2021). Website design and evaluation. In G. Salvendy & W. Karwowski (Eds.), *Handbook of human factors and ergonomics* (5th ed., pp. 1016–1036). Wiley. https://doi.org/10.1002/9781119636113.ch38

Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2024). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*, *31*(5), 1140–1155. https://doi.org/10.1108/JFC-01-2023-0021

Zhang, R., & Volkow, N. D. (2019). Brain default-mode network dysfunction in addiction. *NeuroImage*, *200*, 313–331. https://doi.org/10.1016/j.neuroimage.2019.06.036

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., & Schaub, F. (2020). Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–15). ACM. https://doi.org/10.1145/3313831.3376570