

CYBERCRIME AND GLOBAL PERCEPTION OF NIGERIA'S DIGITAL ECONOMY

Ignatius Ifesinachi Ngini

Department of Political Science
Nnamdi Azikiwe University, Awka
ig.ngini@unizik.edu.ng

ORCID: <https://orcid.org/0009-0007-9465-9795>

Daniel Uchechukwu Lawrence

Department of Political Science
Nnamdi Azikiwe University, Awka
dannyuche2014@gmail.com

ORCID: <https://orcid.org/0009-0005-8278-4455>

Emelife Anthony Mmaduka

Department of Political Science
Nnamdi Azikiwe University, Awka
am.emelife@unizik.edu.ng

ABSTRACT

In an era where digital connectivity defines global participation, Nigeria stands at a crossroads, hailed for its rapid technological adoption yet burdened by the scourge of cybercrime. While the country's youth-led embrace of the digital economy signals immense potential, its growing notoriety as a cybercrime hotspot has tarnished international perceptions and constrained legitimate engagement with its digital economy. Thus, this study critically interrogates how cybercrime shaped global perception of Nigerian digital actors and how this perception affects Nigeria's participation in the global digital economy between 2015 and 2024. Employing an explanatory research design and a mixed-methods approach, the research integrates qualitative data from Key Informant Interviews (KIIs) with law enforcement personnel, cybersecurity experts, academics, financial professionals, and digital entrepreneurs, alongside documentary data from academic literature, official reports, media sources, and social media narratives. Data were analysed using content analysis. Findings reveal that the global digital economy's perception of Nigerian digital actors has been significantly tainted by high-profile cybercrimes, despite the contributions of legitimate digital professionals. This has led to systemic restrictions on Nigerian access to international fintech, freelance, and e-commerce platforms, ultimately stifling innovation, limiting financial inclusion, and deterring foreign investment. The reputational fallout has compromised Nigeria's digital credibility and obstructed its digital economic advancement. The study concludes that while Nigeria aspires to transition from oil dependency to a diversified digital economy, this ambition remains threatened by cybercrime-induced reputational risks. It recommends the urgent development of robust cybersecurity legislation, institutional reforms including a centralized cybercrime task force, nationwide digital ethics education, and the implementation of inclusive digital identity systems. These interventions are essential to restoring global trust and enabling Nigeria's equitable integration into the digital economy.

INTRODUCTION

The rapid spread of information and communications technology (ICT) in this modern age has transformed how individuals, businesses, and governments interact, ushering in a borderless global community marked by unprecedented convenience and efficiency (Abdul-Rasheed, Lateef, Yinusa, & Abdullateef, 2016; Sulaimon, 2024). In Nigeria, this transformation is evidenced by a steep rise in internet subscribers, as the country was ranked 11th globally in internet penetration and 7th in mobile usage (Jaiyeola, 2024; Sulaimon, 2024). Such technological progress forms the foundation of Nigeria's expanding digital economy and underpins Nigeria's ambitions to harness digital technologies for socio-economic development. However, the very developmental milestone that fuels Nigeria's digital economy also exposes it to sophisticated cyber threats.

Cybercrime, defined broadly as illicit activities committed using digital technologies, has evolved into a transnational security concern that no nation, regardless of technological advancement, is immune from (Renu, 2019). In Nigeria, cybercrime commonly referred to as "Yahoo Yahoo" in the local parlance, has escalated alarmingly, particularly among young people in the form of online fraud, identity theft, business email compromise, advance fee fraud, among others (EFCC, 2023; Ojedokun & Ilori, 2021). These illicit practices have generated not only domestic insecurity and economic losses but also substantial damage to Nigeria's international reputation.

Despite state efforts to regulate cyberspace, the continued sophistication of cybercriminals has rendered these responses largely ineffective. The arrest and conviction of young Nigerians in connection with high-profile

scams targeting governments, businesses, and individuals, resulting in losses worth multiple millions of US dollars, have further spotlighted Nigeria in global cybercrime discourse (Ayub & Akor, 2022; BBC, 2022). Recent reports on global cybercrime activities such as the 2023 FBI Internet Crime Report which ranked Nigeria 17th on global sources of cybercrime, with over 1,700 cybercrime complaints, and the 2024 World Cybercrime Index placed Nigeria 5th, reinforce the notion of Nigeria being a hub for cybercrime (Federal Bureau of Investigation, 2023; Bruce et al., 2024). These developments continue to worsen the already struggling global image of the country, which has historically been marred by corruption, human rights abuses, and the involvement of its nationals in transnational crimes such as drug trafficking and money laundering (David, 2021; Owuamanam & Agbaenyi, 2021). The consequence is not only a growing stigmatization of Nigerians globally but also a decline in foreign investor confidence in Nigeria's digital economy, factors that collectively stifle the country's international integration and economic prospects.

The growing size of the global digital economy is opening new opportunities for individuals through remote work, e-commerce, and digital innovation, while enabling countries to diversify their economies and integrate their domestic economy into global value chains for enhanced development and competitiveness. However, many Nigerians are yet to tap fully into these opportunities like their counterparts in developed parts of the world, despite having the skill and knowledge, due to the country's growing association with cybercrime. Nigerian digital entrepreneurs, freelancers, and businesses face barriers in accessing global business platforms, due to restrictive policies designed as a response to widespread fraud concerns coming from the country (Olatunji, 2023; Okamgba, 2024). Consequently, genuine participants in the digital economy suffer collateral damage, further discouraging foreign engagement with Nigeria's online ecosystem. Also, existing literature has largely focused on the general impacts of cybercrime within Nigeria, with limited scholarly attention given to the international implications for Nigeria's image and digital business landscape (Akintaro, 2024; Oni & Oyedokun, 2023). This study thus fills a critical gap by exploring how cybercrime shaped global perception of Nigerian digital actors and how this perception affects Nigeria's participation in the global digital economy between 2015 and 2024.

LITERATURE REVIEW

The advent of cybercrime as a critical global security challenge has raised alarm within criminology and information technology disciplines. Conceptually, cybercrime refers to illegal activities perpetrated through or against computer systems and networks. Scholars such as Ibrahim (2020) and Goni et al. (2022) emphasise that cybercrime includes a broad spectrum of offences ranging from data theft and fraud to hacking and cyber harassment. Bello (2017) and Renu (2019) further categorize these crimes into those targeting individuals, property, and governments, reflecting the complexity and evolving nature of the threat. Importantly, these classifications are echoed in global legal definitions, such as those articulated by the U.S. Department of State and the UK's Crown Prosecution Service, both of which distinguish between cyber-dependent and cyber-enabled crimes (US Department of States, 2015; Crown Prosecution Service, 2022; Crown Prosecution Service, 2024). This consensus reveals a shared understanding that cybercrime, in its many forms, is intricately linked to technological advancement and the vulnerabilities it introduces.

Nigeria's domestic legal response to cybercrime is encapsulated in the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, which criminalizes unauthorized access, data manipulation, and various forms of digital fraud. While this legislative effort represents an important step toward formal regulation, cybercrime remains a persistent issue in Nigeria. Internationally, Nigeria is often viewed as a cybercrime hotspot, a perception exacerbated by high-profile cases such as that of Ramon Abbas (Hushpuppi), whose fraudulent activities drew global media attention. Scholars such as Ayub and Akor (2022) argue that the reputational damage inflicted by such incidents extends beyond individual culpability, contributing to widespread stereotyping of Nigerians as cybercriminals. This perception affects the national image, erodes consumer confidence, and limits foreign investment, despite the growing prominence of Nigeria's digital economy.

The implications of Nigeria's negative cyber reputation are particularly pronounced in its pursuit of integration into the global digital economy. As Adedipe (2016) and Muhammad and Muhammad (2017) observe, Nigeria's burgeoning tech sector and digital entrepreneurship potential are significantly undermined by the international community's mistrust, rooted in cybercrime fears. This mistrust discourages foreign direct investment and forces Nigerian firms to expend resources on damage control rather than innovation. Moreover, perceptions of insecurity in the digital space deter external collaborations and restrict Nigeria's capacity to fully exploit the economic advantages of globalization and ICT proliferation. The resultant diversion of resources towards regulation and reputation management diminishes overall productivity and threatens long-term economic sustainability.

Furthermore, the global perception of Nigeria as a cybercrime epicenter has tangible socio-economic consequences for individual Nigerians, especially in the gig and freelance economies. Researchers such as Ofole (2021), Tunji (2022), and Eleanya (2021) reveal how Nigerian professionals face discrimination in remote work environments due to widespread stereotypes. These include difficulty accessing platforms like PayPal and Fiverr and losing job opportunities upon disclosing their nationality. The restrictions placed on Nigerians by global financial and digital service providers, driven by fears of fraud, inhibit their participation in the global digital economy. While some companies like Flutterwave attempt to bridge these gaps, systemic barriers remain. This marginalization of legitimate Nigerian digital workers and entrepreneurs not only limits income generation but also exacerbates the digital divide.

In addition to external restrictions, the Nigerian government's own measures to combat cybercrime have paradoxically constrained digital economic growth. Olawoyin (2024) highlights the government's decision to block cryptocurrency platforms such as Binance, citing concerns over currency manipulation and illicit finance. While aimed at safeguarding national financial stability, such actions also limit legitimate digital economic activity. Likewise, fraud-related cybercrime has disrupted the development of e-commerce and e-banking in Nigeria. Scholars like Ebenezer et al. (2016) and Enoghomwanse (2019) report that trust erosion has led to reduced e-business transactions, business closures, and diminished foreign investor interest. These challenges underscore the double-edged nature of cybersecurity policies in emerging economies: while regulation is essential, poorly calibrated interventions may stifle innovation and participation in the digital economy.

Despite the dominant narrative positioning Nigeria as a global cybercrime hub, counter-perspectives challenge this assumption. The EFCC (2023) and Ebenezer et al. (2016) argue that the portrayal of Nigeria as a cybercrime epicenter is exaggerated, often shaped by Western media bias. They assert that cybercrime is a global issue, with Western countries experiencing higher volumes and sophistication of fraud. Nonetheless, the persistent negative perceptions continue to harm Nigeria's international standing and economic prospects. Even if cybercrime in Nigeria remains less sophisticated, its visibility and frequency contribute to a harmful stereotype that affects both policy responses and international engagements. Addressing this dual challenge of managing actual cyber threats while reshaping global perceptions is critical for Nigeria's digital economy to thrive.

THEORETICAL FRAMEWORK

This study is anchored on the framework of Kenneth Boulding Image Theory of International Relations. The Image Theory of International Relations, first formally articulated by Kenneth Boulding in a 1958 paper to the American Psychological Association and later expanded in his seminal work *The Image* (1956), highlights the pivotal role of perception in shaping international behaviour. According to Boulding, nation-states do not respond to objective realities but to subjective "images", cognitive representations shaped by historical experience, culture, and ongoing interactions (Boulding, 1959; David, 2021). These mental constructs are not isolated; they form part of collective schemas that guide how states interpret each other's actions and intentions. Boulding argues that these stereotyped perceptions, such as seeing another state as an ally, enemy, or imperialist, profoundly affect foreign policy decisions and diplomatic conduct (Ametbek, 2017; Fontaine, 2010). Hence, international relations become a dynamic arena of interacting images rather than merely strategic interests or material capabilities (David, 2021; Ametbek, 2017).

A key aspect of Boulding's theory is the distinction between "message" and "image." While images are internal mental representations that influence behaviour, messages encompass the external actions, signals, and communications, including diplomacy, media narratives, and people-to-people interactions, that shape or alter these perceptions over time (Ametbek, 2017). This framework gains renewed relevance in the digital era, where national image construction increasingly involves soft power tools such as public diplomacy and global media engagement (Jervis, 1970; Fisher, 1997; Fontaine, 2010). However, the theory has been critiqued for underestimating the influence of domestic political dynamics and national interests on perception formation, and for privileging elite actions over the increasingly significant role of ordinary citizens, particularly in an age where social media amplifies grassroots voices globally. Nonetheless, despite these limitations, Image Theory remains a valuable analytical lens for understanding the psychological and perceptual dimensions of state behaviour in international affairs.

Boulding's Image Theory is relevant to this study as it reveals how entrenched mental stereotypes which cast Nigeria as a hotbed of cybercrime, distort international business engagement and policy responses. Rather than responding to Nigeria's actual digital capabilities or regulatory efforts, international business platforms interpret every action through the pre-existing "scammer" image, which is continuously reinforced by high-profile fraud cases involving Nigerians and global media narratives about Nigeria and cybercrime. In this way, messages, be

they government anti-fraud legislation or legitimate fintech innovations, are filtered through a negative image that undermines trust and skews cost-benefit calculations, deterring investment and Nigeria's access to global digital markets.

METHODOLOGY

The study adopted an explanatory research design to investigate how cybercrime shaped global perception of Nigerian digital actors and how this perception affects Nigeria's participation in the global digital economy. between 2015 and 2024. A mixed-method approach was employed to enhance the depth and credibility of findings. Primary data were collected through Key Informant Interviews (KII) with purposively selected stakeholders, including law enforcement officers, cybersecurity experts, academics, financial institution staff, digital entrepreneurs, and individuals involved in cybercrime, chosen for their experiential knowledge of the subject. Secondary data were drawn from official publications, academic literature, international reports, reputable media sources, and social media narratives, providing a broader context and triangulating insights from the interviews. The data were analysed using content analysis to identify recurring themes, patterns, enabling a comprehensive evaluation of the impact of cybercrime on global perception of Nigerian digital actors and how this perception affects Nigeria's participation in the global digital economy. Ethical considerations such as informed consent, anonymity, and data confidentiality were strictly observed to protect participants and ensure the integrity of the research process.

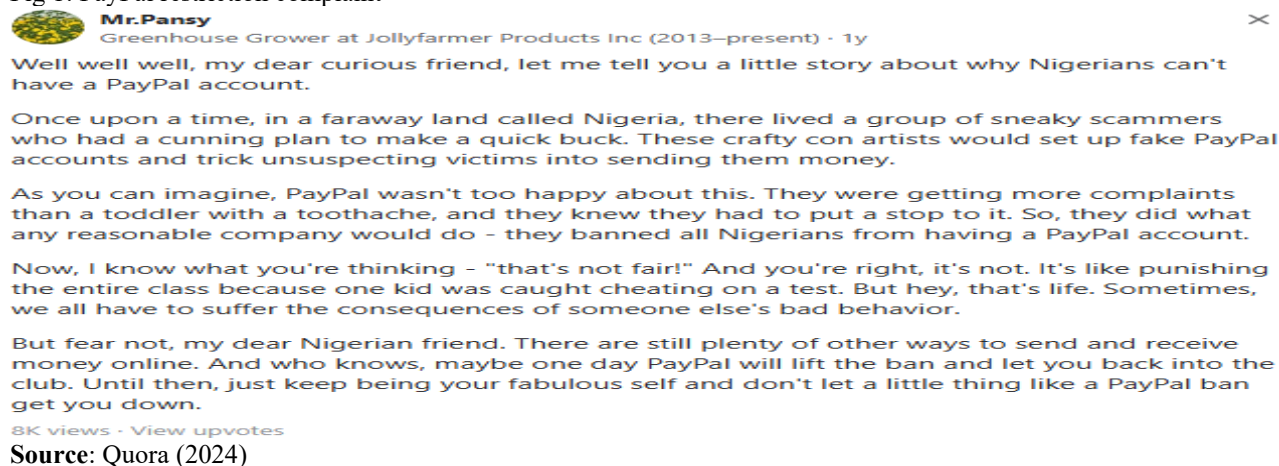
DISCUSSION OF FINDINGS

As the world undergoes rapid digital transformation, new economically lucrative, digitally-driven sectors are emerging to meet a range of human needs, spanning e-commerce, fintech, online education, AI, and more. Nations and individuals are vying to harness the vast opportunities these sectors present. In this context, Nigeria has recently intensified efforts to diversify its oil-dependent economy by engaging with the global digital economy through strategic policies and partnerships. However, this transition is hampered by significant challenges, notably the prevalence of cybercrime. The involvement of some Nigerians in illicit online activities has undermined international trust, deterring potential digital collaborations and investments. This erosion of confidence not only stifles economic growth but also adversely affects law-abiding Nigerian entrepreneurs striving to participate legitimately in the global digital marketplace.

Cybercrime and Restriction of Nigerians on International Financial Technology (fintech) Platforms

In the 21st century, financial technology (fintech) companies have transformed global financial systems by harnessing digital innovation to provide accessible and inclusive financial services to individuals and businesses worldwide, particularly in developing countries. These innovations, ranging from mobile banking and peer-to-peer lending to blockchain, have allowed such nations to overcome traditional banking limitations, significantly advancing financial inclusion and economic participation on a global scale (Bhattacharjee et al., 2024; World Economic Forum, 2024). However, in Nigeria, cybersecurity threats have hindered full access to these global fintech opportunities. Due to persistent fraud concerns and low trust in Nigeria's digital infrastructure, major international fintech firms have imposed limitations on Nigerian users. For example, PayPal, which operates in over 200 countries and supports 25 currencies (PayPal, 2024), has restricted Nigerians from receiving international payments through its platform, a decision influenced by fraud risks, regulatory issues, and currency constraints (Kagan, 2024; Quora, 2024). This restriction curtails the platform's full utility for Nigerians and exemplifies the broader challenges facing fintech access in the country.

Fig 1: PayPal restriction complaint



Global fintech companies such as Wise (formerly TransferWise) and Payoneer have implemented stringent restrictions on Nigerian users largely due to cyberattacks originating from Nigeria, which have resulted in substantial financial losses for individuals and businesses (Tanbasi, 2024). In response to these security threats, Wise limited payment management functionalities for Nigerian users, effectively restricting their ability to receive international transfers through both personal and business accounts. Likewise, Payoneer introduced measures such as withdrawal and transaction limits, restrictions on linking local bank accounts, and increased barriers to account creation for Nigerians (Tanbasi, 2024). While these actions aim to curb fraud-related risks, they have simultaneously constrained legitimate Nigerian users, particularly freelancers, from accessing essential global financial services.

Cybercrime and Transaction Restrictions for Nigerians on Digital Asset Exchange Platforms

Digital assets, encompassing cryptocurrencies, crypto commodities, and crypto tokens—have become a transformative and disruptive element within the contemporary global economic and financial systems, primarily due to their capacity to facilitate rapid, low-cost cross-border transactions that often circumvent traditional banking infrastructures (Library of Congress, 2024; Swiss School of Business and Management, 2024). Supported by blockchain technology and decentralized ledger system, these assets enable secure, peer-to-peer exchanges without central authority intervention, thereby enhancing individual financial autonomy while simultaneously reducing governmental regulatory control (Library of Congress, 2024; Swiss School of Business and Management, 2024). Since the advent of Bitcoin in 2009, and other sub-sequent digital currencies like Ethereum, Ripple, Litecoin, and Dogecoin, the crypto asset ecosystem has expanded significantly, with the total market capitalization of cryptocurrencies exceeding \$1 trillion (Siripurapu & Berman, 2024). This exponential growth has also spurred the emergence of new employment sectors, including positions such as blockchain developers and cryptocurrency analysts (Swiss School of Business and Management, 2024).

The opaque nature of cryptocurrency transactions has intensified concerns over their use in illicit activities, particularly in countries like Nigeria. A significant enforcement action on December 10, 2024, by Nigeria's Economic and Financial Crimes Commission (EFCC), led to the arrest of 792 suspects in Victoria Island, Lagos, for alleged involvement in fraudulent cryptocurrency investments and online romance scams (EFCC, 2024). Among the detainees were foreign nationals from China, the Philippines, Kazakhstan, Pakistan, and Indonesia, as well as Nigerian collaborators trained to impersonate foreign identities and deceive victims, primarily from North America and Europe, into investing on a fraudulent platform, www.yooto.com (EFCC, 2024). EFCC Chairman Ola Olukoyede emphasized the role of digital anonymity in shielding these operations and noted the use of sophisticated computing equipment and foreign lines in executing these scams (EFCC, 2024). This incident reveals broader concerns about the regulatory challenges posed by untraceable crypto transactions.

Considering the persistent scams and illicit uses of crypto assets, the Nigerian government has enacted strict regulatory measures targeting international crypto exchange platforms. These actions date back to January 2017, when the Central Bank of Nigeria (CBN) issued warnings against cryptocurrencies, citing their association with terrorism financing and money laundering (Bakare, 2021). The CBN reiterated its stance in 2018 and in a circular dated February 5, 2021, directed financial institutions to close the accounts of individuals or entities involved in crypto transactions (Bakare, 2021). Following these developments, global exchanges like Binance restricted access to Nigerian accounts, citing fraudulent behavior and implementing compliance mechanisms such as Know Your Customer (KYC) protocols (Azeez, 2022). Tensions escalated further in 2024 when the Nigerian government accused Binance of facilitating illicit capital flows amounting to \$26 billion, leading to website shutdowns and arrests of Binance executives (Adesina, 2024; Odeniyi, 2024). The clampdown culminated in Binance and OKX suspending operations in Nigeria, with OKX officially exiting the market in August 2024 due to regulatory pressures (Okamgba, 2024). These developments have significantly hindered Nigeria's capacity to engage with and benefit from the expanding global digital asset economy.

Impact of Cybercrime on Nigeria's E-Commerce and Freelancing Sectors

Advancements in modern technology have transformed the global business landscape, especially in sectors like e-commerce and freelancing, enabling individuals to offer goods and services globally without physical interaction (Adefioye, 2024). In Nigeria, the rise in mobile phone and internet usage has fueled the expansion of these sectors, significantly contributing to the country's digital economy. However, their growth is increasingly undermined by cybercriminal activities. In particular, the e-commerce sector faces a persistent threat from Nigerian cybercriminals who create counterfeit websites, social media stores, and ads mimicking legitimate businesses to deceive consumers (Adeodun, 2024). Jumia, a major Nigerian e-commerce platform known for its annual Black Friday sales, has often been targeted. During the November 2024 sales, numerous fake Jumia platforms emerged, confusing consumers and resulting in instances of stolen card information and undelivered

purchases, thereby causing substantial financial losses (Balogun, 2024). This experience was shared by an interview respondent, Tsola Duakpenmi:

I have been a victim of fake online store shopping twice, of which I lost money in one. The first experience was on Facebook where I saw a handbag posted on a fake online store of a known female fashion vendor. God being so kind, I was able to avoid making payment for the handbag after I noticed a difference in the account name and the name of the real business owner because I had bought something from her before. However, I was not lucky in my second experience, where I ordered and paid for a lady's shoe (heels) on a fake online store on Instagram pretending to be a known female fashion vendor. I was given two days for it to be delivered to my house in Awka, but the two days passed and I did not receive any package. I called the number displayed on the online store, but it was no longer connecting. I felt very bad because I was a student and then working to support myself in school (*Digital Creator, Lagos, Mobile phone call, January 08, 2025*).

The widespread activities of cybercriminals within Nigeria's e-commerce sector have eroded customer trust, thereby hindering the smooth operation and growth of the industry. Multiple surveys indicate that a significant number of Nigerian online shoppers prefer the Pay-on-Delivery (POD) option over online pre-payment, as a safeguard against fraud (Adedayo, 2017; Agbata, 2019; Giwa, 2022; Ogundimu, 2024). A recent study by the Oxford Business Group supports this trend, revealing that 70 percent of Nigerians opt to pay with cash upon delivery, while only 28 percent use credit or debit cards and a mere 12 percent rely on mobile money platforms (Awodu, 2024). This data aligns with views shared by interviewee Jude Okoye.

There are online stores that will demand you pay for goods before they can be delivered to you. An example is Ali Express because it is part of the company policy. So, Nigerians who use it and those similar to it have no other option but to pay for any goods ordered before they can be delivered even though they may have trust issues, especially those shopping for the first time or have been scammed before. But that is not the case with some other online stores that are in Nigeria which because of competition allow customers who order from them to pay on delivery. Personally, with the way online scams are now rampant, I prefer to pay when I see the product I ordered. Again, some online vendors will display good-looking products in their online stores, but when you order that product, what will be delivered to you will be so different and inferior from what you saw online, after paying so much for it. This is what brought about the slogan that is trending in Nigeria *What I ordered versus what I got*. Because of this, people now prefer to pay when they see what they ordered (*Research Assistant and Data Analyst, Awka, Mobile phone call, January 08, 2025*).

Many online shoppers in Nigeria are reluctant to pay for goods at the point of ordering, a tendency that significantly worsens the financial challenges faced by e-commerce platforms and their affiliated businesses. Instead, customers often choose the "pay on delivery" option, which has led to frequent order cancellations or outright refusal to accept deliveries, often citing various reasons (Adedayo, 2017). These behaviors result in substantial losses for businesses, particularly start-ups, which already invest considerable resources—including time, labor, and logistics costs—into fulfilling such orders (Ogota, 2024). The cumulative effect is a decline in both sales and profit margins, further destabilizing Nigeria's fragile e-commerce ecosystem.

In addition to these challenges, certain unethical practices by Nigerian entrepreneurs on global platforms like Amazon Kindle Direct Publishing (KDP) present another major obstacle to the growth of the country's digital economy. KDP allows authors worldwide, including Nigerians, to publish and distribute their books in various formats without upfront costs while earning royalties (Amazon Kindle, 2024; Umezulike, 2024). However, to maximize financial returns, some Nigerian users have resorted to misconduct such as content plagiarism, copyright violations, algorithm manipulation, and the publication of substandard materials, all of which contravene KDP's guidelines (Umezulike, 2022). These practices, often promoted by online "coaches" who teach exploitative strategies, have led to increased scrutiny and account bans for Nigerian authors, thereby undermining the credibility of genuine publishers and stalling the country's broader digital publishing potential (Umezulike, 2022).

In line with the above stated, Agbo Stephen, a website/mobile application developer, and digital content creator shared an insight on the activities of Nigerians on Amazon Kindle Direct Publishing (KDP):

Before now, it was easy for you to publish your written works on Amazon KDP, especially if you are someone who does not have the money to pay publishing

companies. A good number of Nigerians benefited from Amazon KDP because books are sold in dollars and when you convert your earnings into our local currency, you will have a good amount of money. But the whole thing changed because we Nigerians love money and do not mind cutting corners to get the money. Since publishing on Amazon KDP does not require much process and protocol, some Nigerians began exploiting it. Some were publishing another person's book but will change the cover and put a different name, while the inside content of the book they published is different from the brief description they put out there, and in some cases, the inside content is very scanty. Also, some re-publish a book they have published before using a different title, book cover design, and a Western author name that does not exist anywhere. Again, some write books on areas they have no professional or academic knowledge of using Artificial Intelligence (AI) (*Website/mobile application developer, and Amazon KDP Publisher, Enugu, WhatsApp communication, May 03, 2024*).

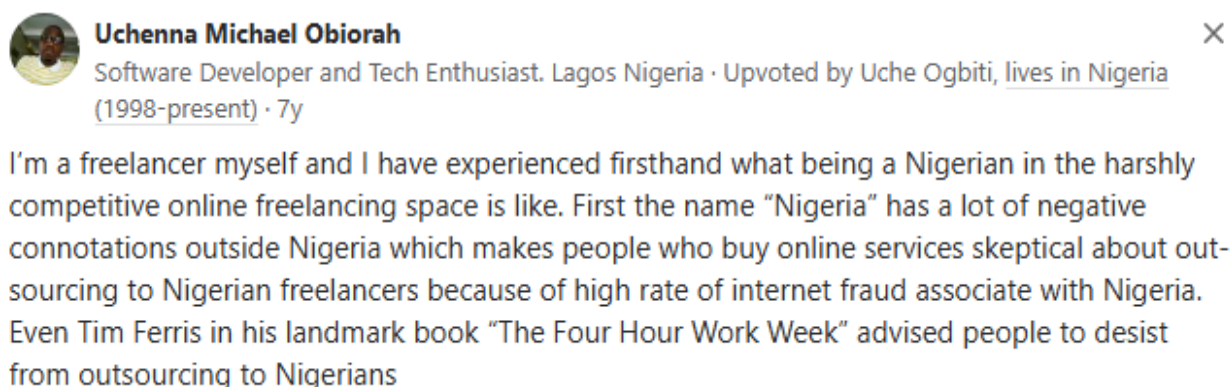
The interview respondent went further to expose how genuine publishers from Nigeria have been affected by the criminal activities of some Nigerians on Amazon KDP.

Currently, Nigerians have a bad reputation on Amazon KDP and to publish a book on the platform as a Nigerian user is no longer as easy as it was some years back. Even as a new person from Nigeria on the platform, creating a new account is quite challenging. Some Nigerians now use a foreign identity to create accounts and publish books to avoid the ban and serious scrutiny Nigerian users now face on Amazon KDP all because of the inappropriate behaviours of some of us. All of us have been negatively, especially in the area of maximising the economic benefits and visibility the platform gives genuine writers (*Website/mobile application developer, and digital content creator, Enugu, WhatsApp communication, May 03, 2024*).

The growth of e-commerce in Nigeria has been considerably hindered by cyber-related criminal activity, which has disrupted the sector's once-optimistic trajectory. From a promising valuation of \$12 billion in 2016 and \$13 billion in 2017, the industry suffered a sharp decline to \$5 billion by 2020. Even as revenue rose to \$7.6 billion in 2021, it dropped again to \$6.2 billion by 2022, underscoring the volatility and vulnerability of the digital marketplace (Abisoye, 2017; Anuforo, 2018; Clement, 2022; Oxford Business Group, 2024). Nonetheless, the industry has shown signs of recovery, with an estimated valuation of \$9 billion in 2023 and a projected increase to \$14.6 billion by 2024, suggesting a degree of resilience and latent potential within the sector despite ongoing challenges (Aimuengheuwa, 2024; Research and Markets, 2024).

At the same time, the freelance (gig) economy has flourished amid the broader digital transformation of the 21st century, enabling freelancers to work independently for various clients without formal employment commitments. This model thrives particularly in skill-based sectors such as copywriting, software development, engineering, and digital marketing (The Upwork Team, 2024). According to the World Bank, Nigeria, Kenya, and South Africa collectively account for 80.6% of Sub-Saharan Africa's freelance market, with 17.5 million active online gig workers (Jaiyeola, 2023). However, Nigerian freelancers are facing increasing marginalization on major platforms like Fiverr, Freelancer, and Upwork, where they encounter both algorithmic invisibility and client prejudice due to the country's association with cybercrime (Business Elite Africa, 2024). For instance, Fiverr has been accused of limiting the visibility of Nigerian freelancers, even those with stellar reputations and thousands of positive reviews (Olatunji, 2023). This has led to frustration among diligent Nigerian freelancers whose livelihoods are being affected by systemic bias and entrenched stereotypes, further perpetuated by prior fraud cases and negative public discourse (Sangoleye, 2018; Quora, 2021).

Fig. 2: Complaint about negative stereotypes against Nigerian freelancers by a Nigerian software developer and tech enthusiast



Source: Quora (2021)

Fig. 3: A Nigerian X (Formerly known as Twitter) user complaining of being blocked by a potential client on Upwork after being accepted for a job for revealing her identity as a Nigeria



Source: Nigerian Bulletin (2024)

The general distrust toward Nigerian freelancers, largely stemming from the association of some Nigerians with cybercrime, has significantly hindered their ability to secure jobs and results in lower pay compared to freelancers from other countries. According to a recent study by Bookipi, Nigerian freelancers rank 18th out of 40 countries on Upwork in terms of pricing, charging an average of \$163 per job, while their counterparts in Australia, India, and Morocco earn \$594.56, \$501.00, and \$402.03 per job, respectively (Akintaro, 2024). This pervasive skepticism in the global digital market not only tarnishes the reputation of Nigerian professionals but also undermines international confidence in Nigeria's digital economy, potentially stalling partnerships and investments, despite the sector's notable growth from \$5.09 billion in 2019 to \$9.97 billion in 2021, with projections reaching \$18.30 billion by 2026 (Agbola, 2022). This aligns with the thoughts of an interview respondent, Chukwuebuka C. Ume-Ezeoke:

Cybercrime deters potential foreign investors due to concerns about the security of their and the overall business environment. Mistrust in transactions involving Nigerians can limit their participation in global e-commerce, as international partners may hesitate to engage due to fear of fraud (Cybersecurity expert at CED Technologies, London, United Kingdom, LinkedIn communication, July 17, 2024).

The above submissions call for urgent intervention by relevant stakeholders to address the threat posed by cybercriminals, which undermines Nigeria's economic benefits and potential, as the International Trade Association (2024) affirms that cybercrime remains a significant obstacle to the projected growth of Nigeria's digital economy and the inclusion of Nigerians in the vast and evolving global digital landscape.

CONCLUSION

While Nigeria has made commendable strides toward embracing the global digital economy as a means of diversifying its oil-dependent economy, the pervasive threat of cybercrime continues to severely undermine these efforts. The negative global perception generated by the activities of a minority of Nigerian cybercriminals has led to widespread restrictions on the country's access to international fintech, digital asset exchange, e-commerce, and freelance platforms. These restrictions, although intended to safeguard global digital platforms from fraud and abuse, have inadvertently marginalized legitimate Nigerian entrepreneurs, professionals, and digital creators, stifling innovation, restricting financial inclusion, and reducing international investment

opportunities. The resulting reputational damage erodes global confidence in Nigeria's digital infrastructure and regulatory credibility, posing a significant barrier to its digital economic aspirations.

RECOMMENDATIONS

Thus, to fully harness the transformative potential of the digital economy, this study recommends:

1. The Nigerian government, in collaboration with relevant international and private-sector stakeholders, should prioritize the development and enforcement of comprehensive cybersecurity legislation and standards. This should include the creation of a centralized cybersecurity task force empowered to detect, investigate, and prosecute cybercrimes efficiently. Emphasis must also be placed on transparency, regular audits, and real-time threat intelligence sharing to restore trust among global digital platforms and investors.
2. Further, to address the root causes of cybercriminal behaviour and promote a culture of digital responsibility, the government should initiate nationwide digital ethics and cybersecurity awareness campaigns. These should be integrated into educational curricula from secondary school through tertiary levels, and supplemented with public campaigns targeting digital entrepreneurs, freelancers, and e-commerce users. Strategic partnerships with tech companies and civil society organizations can aid in delivering impactful, community-based education.
3. Lastly, the government and private-sector actors should invest in the development and mandatory integration of secure digital identity and Know Your Customer (KYC) verification systems across all digital platforms. These systems should be user-friendly and inclusive to encourage compliance among freelancers, online vendors, and fintech users.

REFERENCES

- Abdul-Rasheed, S. L., Lateef, I., Yinusa, M. A., & Abdullateef, R. (2016). Cybercrime and Nigeria's external image: A critical assessment. *Africology: The Journal of Pan African Studies*, 9(6), 119–132.
- Abisoye, O. (2017, June 23). Nigeria's \$12bn e-commerce market seen as driver of growth in near term. *Businessamlive*. <https://www.businessamlive.com/nigerias-12bn-e-commerce-market-seen-driver-growth-near-term/>
- Adedayo, T. (2017, March 27). The good, the bad, the demerits of Payment on Delivery (POD) in Nigeria's E-commerce space. *Medium*. <https://medium.com/@toluwaseadedayo/the-good-the-bad-the-demerits-of-payment-on-delivery-pod-in-nigerias-e-commerce-space-166fa2f9bbd9>
- Adedipe, A. A. (2016). *Nigerian internet fraud: Policy/law changes that can improve effectiveness* (Publication No. 803). Regis University Student Publications. <https://epublications.regis.edu/theses/803>
- Adefioye, A. (2023, July 21). Why e-commerce is better: E-commerce vs freelancing. *Illumination*. <https://medium.com/illumination/why-e-commerce-is-better-e-commerce-vs-freelancing-be6481af1165>
- Adeodun, A. (2024, March 31). Online shopping scams: A growing threat in Nigeria. *NewsSociety*. <https://inquirer.ng/2024/03/31/online-shopping-scams-a-growing-threat-in-nigeria/>
- Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science*, 13(4), 19–29.
- Agbata, C. F. (2019, January 27). What is wrong with e-commerce in Nigeria? *Punch Nigeria*. <https://punchng.com/what-is-wrong-with-e-commerce-in-nigeria/>
- Agboola, O. (2022). Nigeria's budding digital economy: Coping with disruptive technology. *Central Bank of Nigeria Economic and Financial Review*, 60(4), 33–50. <https://www.cbn.gov.ng/out/2024/rsd/nigeria%E2%80%99s%20budding%20digital%20economy.pdf>
- Aimuengheuwa, J. (2024, October 21). The future of e-commerce in Nigeria: Trends and challenges. *Tech Economy*. <https://techeconomy.ng/the-future-of-ecommerce-in-nigeria-trends-and-challenges/>
- Akintaro, S. (2024, April 12). Nigeria ranks 5th in global cybercrime index. *Nairametrics*. <https://nairametrics.com/2024/04/12/nigeria-ranks-5th-in-global-cybercrime-index/>
- Akintaro, S. (2024, April 17). Freelancing: Nigerians among least expensive workers on Upwork – Report. *Nairametrics*. <https://nairametrics.com/2024/04/17/freelancing-nigerians-among-least-expensive-workers-on-upwork-report/>
- Ametbek, D. (2017, June 24). Perception and image theory of international relations. *Ankara Centre for Crisis and Policy Studies*. <https://www.ankasam.org/perception-and-image-theory-of-international-relations/?lang=en>
- Anuforo, C. (2018, May 28). Nigeria's e-commerce sector struggles despite growth potential. *The Sun Nigeria*. <https://thesun.ng/nigerias-e-commerce-sector-struggles-despite-growth-potential/>

- Awodu, R. (2024, April 20). Empowering Nigerian retail: The promise of pay on delivery. *BusinessDay*. <https://businessday.ng/bd-weekender/article/empowering-nigerian-retail-the-promise-of-pay-on-delivery/>
- Ayub, A. O., & Akor, L. (2022). Trends, patterns and consequences of cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences*, 5(1), 241–262.
- Bakare, A. (2021, February). Cryptocurrency trading: CBN orders banks to close operating accounts. *CBN Update*, 3(2), 1–14. <https://www.cbn.gov.ng/out/2021/ccd/volume%203%20number%202%20cbn%20update%20february%202021.pdf>
- Balogun, M. (2024, November 21). Exposing eight Facebook pages posing as popular Nigerian online store Jumia to offer fake ‘Black Friday’ deals. *Africa Check*. <https://africacheck.org/fact-checks/meta-programme-fact-checks/exposing-eight-facebook-pages-posing-popular-nigerian-online>
- BBC. (2022, November 8). Hushpuppi: Notorious Nigerian fraudster jailed for 11 years in US. <https://www.bbc.com/news/world-africa-63542573>
- Bello, A. T. (2017, October 19). Anatomy of Cybercrime in Nigeria: The Legal Chronicle. *Social Science Research Network (SSRN)*. <http://dx.doi.org/10.2139/ssrn.3055743>
- Bhattacharjee, I., Srivastava, N., Mishra, A., Adhav, S., & Singh, N. (2024). The rise of fintech: Disrupting traditional financial services. *Educational Administration: Theory and Practice*, 30(4), 89–97. <https://doi.org/10.53555/kuey.v30i4.1408>
- Boulding, K. E. (1959). National images and international systems. *Journal of Conflict Resolution*, 3(2), 120–131. <https://doi.org/10.1177/002200275900300204>
- Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE*, 19(4), e0297312. <https://doi.org/10.1371/journal.pone.0297312>
- Business Elite Africa. (2024). Great freelance platforms in Nigeria you probably don’t know about. <https://businesselitesafrica.com/great-freelance-platforms-in-nigeria-you-probably-dont-know-about/?v=66e10e9ff65e>
- Crown Prosecution Service (2022). *Cyber/online crime*. United Kingdom’s Government <https://www.cps.gov.uk/crime-info/cyber-online-crime#:~:text=drugs%20and%20firearms,-Cybercrime,or%20simply%20to%20disrupt%20businesses>.
- Crown Prosecution Service (2024). *Cybercrime - prosecution guidance*. United Kingdom’s Government. <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>
- David, I. (2021). Nigeria’s image problem and image-polishing: Foreign policy responses since 1999. *African Studies Quarterly*, 20(4), 41–55. <https://asq.africa.ufl.edu/wp-content/uploads/sites/168/V20i4a3-1.pdf>
- Ebenezer, A. J., Paula, A. M., & Allo, T. (2016). Risk and investment decision making in the technological age: A dialysis of cyber fraud complication in Nigeria. *International Journal of Cyber Criminology*, 10(1), 62–78. <https://doi.org/10.5281/zenodo.58522>
- Economic and Financial Crimes Commission (EFCC). (2023, December 5). EFCC presents N76.586 billion budget proposal to House of Reps. <https://www.efcc.gov.ng/efcc/news-and-information/news-release/9645-efcc-presents-n76-586-billion-budget-proposal-to-house-of-reps>
- Economic and Financial Crimes Commission (EFCC). (2024). Red Alert on Scam. <https://www.efcc.gov.ng/efcc/records-3/red-alert/red-alert-on-scam>
- Economic and Financial Crimes Commission (EFCC). (2024, December 16). EFCC bursts syndicate of 792 cryptocurrency investment, romance fraud suspects in Lagos ... Arrests 193 Chinese, Arabs, Filipinos, Others. <https://www.efcc.gov.ng/efcc/news-and-information/news-release/10584-efcc-bursts-syndicate-of-792-cryptocurrency-investment-romance-fraud-suspects-in-lagos-arrests-193-chinese-arabs-filipinos-others>
- Eleanya, F. (2021, March 23). For PayPal and Flutterwave, road to unite Africa’s payment system opens. *BusinessDay*. <https://businessday.ng/lead-story/article/for-paypal-and-flutterwave-road-to-unite-africas-payment-system-opens/>
- Enoghomwanse, A. (2019). Cybercrime and its economic impact in Nigeria. *South Eastern Journal of Research and Sustainable Development*, 2(1), 16–31.
- Federal Bureau of Investigation. (2023). *2023 Internet Crime Report*. Internet Crime Complaint Center (IC3). https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
- Fisher, G. (1997). *Mindsets: The role of culture and perception in international relations* (2nd ed.). Intercultural Press.
- Fontaine, P. (2010). Stabilizing American society: Kenneth Boulding and the integration of the social sciences, 1943–1980. *Science in Context*, 23(2), 221–265. <https://doi.org/10.1017/S0269889710000050>

- Giwa, T. (2022, February 21). Why pay on delivery is the worst thing to happen to e-commerce in Nigeria. *Medium*. <https://medium.com/the-startup-hacker/pay-on-delivery-the-worst-thing-to-happen-to-e-commerce-614bd68c81b1>
- Goni, O., Ali, M. H., Showrov, A. M. M., & Shameem, M. A. (2022). The basic concept of cybercrime. *Journal of Technology Innovations and Energy*, 1(2), 29–39.
- Ibrahim, U. (2020). The impact of cybercrime on the Nigerian economy and banking system. *Nigeria Deposit Insurance Corporation Quarterly*, 34(12), 1–20. <https://demo.ndic.gov.ng/wp-content/uploads/2020/08/NDIC-Quarterly-Vol-34-No-12-2019-Article-The-Impact-Of-Cybercrime-On-The-Nigerian-Economy-And-Banking-System.pdf>
- International Trade Administration. (2024, September 18). National Focus: Government digital economy/growth/transformation plans or strategies. Nigeria - Country Commercial Guide. <https://www.trade.gov/country-commercial-guides/nigeria-digital-economy>
- Jaiyeola, T. (2023, September 12). Nigeria, others have 17.5 million online freelancers, says W'Bank. *Punch*. <https://punchng.com/nigeria-others-have-17-5-million-online-freelancers-says-wbank/>
- Jaiyeola, T. (2024, March 19). Nigeria's internet usage up 38% on smartphone uptake. *Business Day*. <https://businessday.ng/technology/article/nigerias-internet-usage-up-38-on-smartphone-uptake/>
- Jervis, R. (1970). *The logic of images in international relations*. Princeton University Press.
- Kagan, R. (2024). *The cost of American global leadership*. Brookings Institution Press.
- Library of Congress. (2024). *Country profile: Nigeria*. <https://www.loc.gov/>
- Muhammad, A., & Muhammad, A. (2017). Cybercrime and its implications for Nigeria's economic and financial sectors. *Journal of Social and Management Sciences*, 15(1), 24–35.
- Odeniyi, S. (2024, August 27). Binance CEO demands release of employee detained in Nigeria. *Punch*. <https://punchng.com/binance-ceo-demands-employee-release-from-nigerian-custody/>
- Ofole, J. E. (2021). Why is Fiverr so strict with Africans especially Nigerians these days? Nigerians are smart and they work hard, why is Fiverr making it hard for them? *Quora*. <https://www.quora.com/Why-is-Fiverr-so-strict-with-Africans-especially-Nigerians-these-days-Nigerians-are-smart-and-they-work-hard-why-is-Fiverr-making-it-hard-for-them>
- Ogota, G. (2024, October). Rising fraud threatens e-commerce growth in Nigeria—Experts. *Geesix*. <https://geesixglobal.com.ng/rising-fraud-threatens-e-commerce-growth-in-nigeria-experts/>
- Ogundimu, A. (2024, March 27). Cash-on-delivery: Obstacles and benefits. *Daily Trust*. <https://dailytrust.com/cash-on-delivery-obstacles-and-benefits/#:~:text=One%20of%20the%20primary%20reasons,for%20non%2Ddelivery%20of%20items>
- Ojedokun, U. A., & Ilori, A. A. (2021). Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria. *International Journal of Criminal Justice*, 3, 1–24.
- Okamgba, J. (2024, July 18). OKX crypto exchange exits Nigeria amid regulatory crackdown. *Punch*. <https://punchng.com/okx-crypto-exchange-exits-nigeria-amid-regulatory-crackdown/>
- Olatunji, K. (2023, October 19). Facing the blacklist: An insider's look into discrimination against Nigerians on freelancing platforms. *Medium*. <https://medium.com/@kayodej4/facing-the-blacklist-an-insiders-look-into-discrimination-against-nigerians-on-freelancing-e82272a1086a>
- Olawoyin, O. (2024, February 21). Forex crisis: Nigerian govt blocks Binance, OctaFX, Coinbase, others. *Premium Times*. <https://www.premiumtimesng.com/business/670511-forex-crisis-nigerian-govt-blocks-binance-octafx-coinbase-others.html?tztc=1>
- Oni, S. O., & Oyedokun, G. E. (2023). Adopting cryptocurrency in Nigeria: Tax, legal and financial implications. *ResearchGate*. https://www.researchgate.net/publication/373598276_adopting_cryptocurrency_in_nigeria_tax_legal_and_financial_implications
- Owuamanam, C. M., & Agbaenyi, A. N. (2021). Nigeria's international image crisis: An evaluative analysis. *Zik Journal of Multidisciplinary Research*, 4(1), 99–115. <https://journals.aphriapub.com/index.php/ZJMR/article/view/1373>
- Oxford Business Group. (2024). Booming population and e-commerce in Nigeria spur innovation in retail. <https://oxfordbusinessgroup.com/reports/nigeria/2024-report/retail/on-the-up-a-booming-population-and-the-rapid-rise-of-e-commerce-creates-opportunities-for-disruption-and-innovation-overview/>
- PayPal. (2024). We get where you are coming from. <https://www.paypal.com/fo/webapps/mpp/country-worldwide#:~:text=We%20are%20available%20in%20more,over%20borders%20and%20language%20barriers>
- Quora. (2021). Why is it hard for Nigerian developers to get jobs on online freelancing sites? <https://www.quora.com/Why-is-it-hard-for-Nigerian-developers-to-get-jobs-on-online-freelancing-sites>
- Renu, P. (2019). Impact of cybercrime: Issues and challenges. *International Journal of Trend in Scientific Research and Development*, 3(3), 1569–1572.

- Research and Markets. (2024, July 10). Nigeria ecommerce market databook 2024: 100+ KPIs on ecommerce verticals, market share by key players, sales channel analysis, payment instrument, consumer demographics 2019–2028. *Business Wire*.
<https://www.businesswire.com/news/home/20240710856252/en/nigeria-ecommerce-market-databook-2024-100-kpis-on-ecommerce-verticals-market-share-by-key-players-sales-channel-analysis-payment-instrument-consumer-demographics-2019-2028---researchandmarkets.com>
- Sangoleye, F. (2018, October 16). 5 challenges of a Nigerian freelancer. *Medium*.
<https://medium.com/techloy/challenges-of-a-nigerian-freelancer-cfa3453d5b1c>
- Siripurapu, A., & Berman, N. (2024, January 17). The crypto question: Bitcoin, digital dollars, and the future of money. *Council on Foreign Relations*. <https://www.cfr.org/background/crypto-question-bitcoin-digital-dollars-and-future-money>
- Sulaimon, A. (2024, February 24). FULL LIST: Lagos, Kaduna, others top Nigeria's internet users. *Punch*.
<https://punchng.com/full-list-lagos-kaduna-others-top-nigerias-internet-users/>
- Swiss School of Business and Management. (2024, April 7). How cryptocurrencies are changing the business landscape. *Swiss School of Business and Management Geneva*. <https://www.ssbm.ch/how-cryptocurrencies-are-changing-the-business-landscape/>
- Tanbasi, S. (2024, July 24). How to receive payment from international clients as a freelance marketer in Nigeria. *Smartermarketers*. <https://www.smartermarketershub.com/blog/receive-international-payment-in-nigeria#:~:text=Payoneer&text=Limited%20receiving%20options%3A%20While%20Nigerians,trans action%20amounts%20or%20withdrawal%20methods>
- The Upwork Team. (2024, August 12). What is freelancing? Basics and popular jobs in 2025. *Upwork*.
<https://www.upwork.com/resources/what-is-freelancing>
- Tunji, S. (2022, August 17). High unemployment drives cybercrime in Nigeria - Expert. *Punch*.
<https://punchng.com/high-unemployment-drives-cybercrime-in-nigeria-expert/>
- Umezulike, S. (2022, July 23). Here is why amazon is banning lots of Nigerian accounts on their KDP platform. *Branditechture*.
<https://branditechture.agency/heres-why-amazon-is-banning-lots-of-nigerian-accounts-on-their-kdp-platform/>
- Umezulike, S. (2024). Corruption in Nigeria: Patterns and trends. Third survey on corruption as experienced by the population. United Nations Office on Drugs and Crime (UNODC).
https://track.unodc.org/uploads/documents/corruption/Publications/2025/UNODC_Corruption_in_Nigeria_-_patterns_and_trends_2024.pdf
- United States Department of State. (2015). Cybercrime. Office of the Coordinator for Cyber Issues (S/CCI).
<https://2009-2017.state.gov/documents/organization/255007.pdf>
- World Bank. (2023). Poverty & equity brief Africa Western & Central: Nigeria.
https://databankfiles.worldbank.org/public/ddpext_download/poverty/987B9C90-CB9F-4D93-AE8C-750588BF00QA/current/Global_POVEQ_NGA.pdf
- World Economic Forum. (2024, February 16). Fintech is growing fast. Here are 3 reasons why that's a good thing. <https://www.weforum.org/stories/2024/02/fintech-growth-customer-demand/>