International Journal of Advanced Research in Public Policy, Social Development and Enterprise Studies
p-ISSN: 2536-6548 | e-ISSN: 2536-6556

IJARPPSDES

June, 2024
Vol. 5, No. 1

Covid-19 Lockdown and Spike in Yahoo Activities in Nigeria

[1]Ene, Warikiente Robert & [2]Otobo Irene Odion
[1&2]Department of Sociology and Anthropology
Faculty of Social Sciences, Federal University Otuoke

Article DOI:
10.48028/iiprds/ijarppsdes.v5.i1.08

Abstract

The aim of this study is to examine the impact of the COVID-19 Lockdown on the prevalence of Yahoo Activities in Nigeria. The work seeks to deepen our understanding of the socio-economic conditions enabled by the Covid-19 which may have bred a surge in Yahoo activities and its dynamics with a view to providing more robust remedial insights to stakeholders and policy makers. In a bid to achieve these objectives, the study utilized the Anomie and Strain Theories using Qualitative Research method. In this light, it engaged textual analysis of secondary data of documentary works sourced from the internet and library. The result indicates positive correlation between COVID-19 lockdown and surge in Yahoo Activities. The findings show that the increased online activity (i.e. of individuals and businesses) due to the lockdown propelled many Yahoo boys to intensify their online activities given the relative dominance of the virtual society of the time. Also, the socio-economic hardship and unemployment occasioned by the lockdown, pushed many young persons into the act, all contributing to the upsurge. There is an indication that the surge will not dwindle after the lockdown and therefore, may pose more socio-economic damage to the country. To this end, an urgent and a multi-pronged approach that includes law enforcement, technological advancement, public awareness and industry collaboration is essential to address the threats of the fast-spreading Yahoo activities.

Keywords:
COVID-19, Lockdown, Yahoo, Yahoo activities, Nigeria

Corresponding Author:
Ene, Warikiente Robert

Background to the Study

The global COVID-19 pandemic brought unprecedented impact on almost every aspect of lives. While health and safety are often the focus of attention, other aspects have also been affected, including crime rates such as internet fraud, commonly referred to as 'Yahoo'. Due to the highly contagious nature of COVID-19, infection rates increased globally (Rothan & Byrareddy, 2020). As a result, the World Health Organization (WHO) declared the outbreak of COVID-19 a global pandemic on March 11, 2020 and many countries implemented lockdowns as an effective measure to control the spread of the virus. In Nigeria, the index case of the disease was recorded by the Nigeria Center for Disease Control on 27th February 2020 (NCDC Report, 2020). From then, the spread of the disease continued unabated, killing hundreds of people in the country. The country was severely affected by the devastating effects of the virus. Due to the above, the Nigerian government initiated a lockdown to flatten the curve of the infection.

Expectantly, the COVID-19 lockdown initiatives reconfigured and reconstructed our social structures and environments. With stay-at-home orders, travel bans and social distancing regulations, internet usage increased as people rely on online platforms for banking, healthcare, entertainment, business, education and essential government services (Hakak et al, 2020). Many people also transitioned from working in an office setting to working from home, rely on online shopping, engage in virtual social events or dating instead of visiting friends or getting to know new people in the real world. As the public shifts from in-person activities to online activities, Yahoo boys seized the opportunity by moving their activities into cyberspace, resulting in service disruptions, financial losses, data breaches, and personal and institutional fears (Hakak et al., 2020).

Studies have shown an increase in Yahoo Boy activity during that time. For example, in March, phishing and hacking attacks and threats were five to six times higher than usual (Kumaran and Lugani, 2020). By the end of March, more than 42,000 websites had been registered with domains containing "COVID" and "corona," many of which appear suspicious (Kumaran & Lugani, 2020). Researchers also observed a significant 667% increase in COVID-19 phishing messages (Shi, 2020). Between March 1 and March 23, there were more than 9,000 email attacks related to COVID-19, compared to 1,188 in February and 137 in January (Shi, 2020). In April, the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) received between 3,000 and 4,000 cybersecurity complaints per day, up from an average of 1,000 per day before COVID-19 (Cimpanu, 2020).

In recent time, internet fraud or cybercrime is increasingly visible in the activities of Yahoo Guys these days (Lazarus & Button, 2023). These boys are young men with education and access to the Internet, most of whom live in large cities (Joseph and Afolabi, 2020). According to Sesan, Soremi and Olufemi (n.d.), as a result of access to modern technology, Yahoo boys engage in various criminal activities for economic gains. Joseph and Afolabi (2020), revealed that their modus operandi consists of sending emails, using various social media platforms, falsifying their identity to harass victims and posing as

lovers, businessmen or contractors with the intention to defraud (Oloworekende, 2019). Regrettably, their activities have tarnished the image of the country and destroyed the goodwill of hardworking and enterprising Nigerians globally (Joseph & Afolabi, 2020). Ogundele, et al. (2023), posited that the activities of Internet fraudsters and Yahoo have constituted a major problem in Nigerian society today because Internet fraud is a criminal act with reputational and economic consequences for the country. The actions of Yahoo boys have resulted in financial losses for individuals and placed Nigeria in the spotlight for crime in the national community.

The rise in internet fraud in the country has been attributed to a number of structural, systemic and economic factors. Most of those responsible for these questionable scandals blame the flawed political and economic systems that leave the country's citizens hungry. Rapid increases in poverty rates, youth unemployment, lack of economic opportunities, failing education systems, hardship and corruption have forced the youth, the population most affected by these woes, to embrace the latest ICT for crimes such as internet fraud (Adeniran, 2008). The exaggerated and unsavory behavior of the Yahoo Boys, also known as benefit Boys, G Boys and Big Boys, which comes with a huge benefit captor mentality (Raimi, 2017) has attracted national and international attention. Their criminal activities led former US Secretary Collins Powell to describe Nigeria as a "nation of thieves" (Glickman, 2013, 3). Although yahoo activities predate the covid-19 era, the pandemic instigated a spike and can sustained a growing posture in subsequent years if not tamed. This will invariable compound the problems that Nigeria is battling with such as insecurity, corruption etc.

Many studies have been carried out to the adverse effects of the pandemic on different aspects of life. For instance, Kumar and Nayar (2020) and Lee (2020) assessed the impact of COVID-19 on psychological and mental health; Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple and Bellekens (2021) examined the timeline and analysed cyber-crime and cyber-attacks during the Pandemic; Kumaran and Lugani (2020) studied cyber threats on businesses during COVID-19; Rothan and Byrareddy (2020), looked at the epidemiology and pathogenesis of the pandemic outbreak and Naidoo (2020) carried out a multi-level Influence model of COVID-19 themed cybercrime. While these studies shed light on the different shades impacts of the pandemic, there are little or no work carried out specially, to establish how COVID-9 contributed to the rise in the incidence of yahooboys activities in Nigeria. Thus, this study seeks to fill this gap by examining the relationship between the COVID-19 lockdown and the spread of Yahoo activities in Nigeria. This study addresses this complex issue of fraud and provides a deeper understanding of the changing landscape of Internet fraud in these challenging times, with the aim of enabling relevant stakeholders to adopt a comprehensive remedial approach.

Objectives of the Study

To this paper is guided by the following objectives;

i. To examine the influence of COVID-19 LOCKDOWN on the Spike in Yahoo Boys

activities in Nigeria.

ii. To assess the prevalence of Yahoo boys' activities during the COVID-19 LOCKDOWN mandate in Nigeria.
iii. To investigate how the COVID-19 LOCKDOWN made people vulnerable to Yahoo boy's activities in Nigeria.

Conceptual Clarification

COVID-19: An abbreviation created by the World Health Organization (WHO), meaning coronavirus disease 2019. It is an infectious disease caused by severe acute respiratory syndrome. Coronavirus primarily targets the human respiratory system (Rothan & Byrareddy, 2020). Respiratory infections are transmitted primarily through contact, droplets, and airborne transmission (Centers for Disease Control and Prevention, 2020).

Literature Review

History of Yahoo (Internet Scam) in Nigeria

Yahoo boys are online scammers who got their name from the Yahoo email service, which gained prominence in Nigeria in the 2000s. The activities of fraudsters, commonly known as "Yahoo Boys", are not a recent phenomenon in the history of Nigeria (Ezea, 2017). Although, the pervasive nature of the internet has extended its reach and manifestation, the history of fraudsters predates the days of the internet. Its intensity and prevalence indicate the evolution of today's society, where crime has become more sophisticated and technologically advanced (Lazarus & Button, 2023; Ayodele, 2021; Asemota, et al, 2016). Ezea (2017) added that the activities of fraudsters were common in major Nigerian cities such as Lagos in the 1990s and were known as "419-ners". These individuals at that time, before the liberalization of internet technology or the availability of personal computers used fax machines to fraudulently extort money from both foreigners and Nigerians using various "make believe" schemes. Demographically, the 419 individuals and fraudsters included both educated and uneducated adult males and females.

Furthermore, Ezea (2017) avers that the rise of financial fraud among youths in Nigerian society in the 1990s is a striking indication of the social breakdown of the country's moral value system. This created a situation in which wealth without known source or without hardwork is celebrated. Thus, the swindler became a man who became a symbol of attention, respect and wealth of the nation. The likes of Emmanuel Nwude were among those celebrated but was later arrested and charged by Nigeria's anti-corruption agency. Arguably, he and others sowed the seeds of fraud, which became a garden of great social problems for the country, its economy and image.

Olawoyin (2021) pointed out that before the emergence of internet fraudsters known as Yahoo Boys, the first wave of fraudsters in Nigeria consisted of uneducated individuals who used fraud as an escape or survival mechanism to cope with the depressed economy in the 1990s. The current economic situation and the unemployment rate have not changed significantly. Therefore, Internet fraud or Yahoo Yahoo has become a common activity among most Nigerian youths. Just as in the past, before the Internet became

popular, financial fraud was associated with unfavorable economic conditions in countries, this remains true even today.

Several factors have recently exacerbated Nigeria's digital crisis and widespread cyber fraud and crime. The emergence and easy accessibility of the Internet, volatile moral and decaying value systems, the collapse of social institutions such as the family, school, church, mosque, etc., the worsening economic situation that glorifies poverty and COVID-19, lead to internet fraud. Ezea (2017) added that the prevalent nature of internet scams among Nigeria youth especially undergraduates, secondary school leavers can be traced to the introduction of the internet and its related technologies. Internet fraud or the colloquially dubbed "yahoo yahoo" utilised the use of email accounts such as the Yahoo mail to send dishonest messages that target victims either through promise of love or businesses to defraud them.

Muhammad (2022) noted that several Yahoo groups have emerged in Nigeria over time. The first group, which began operating in the early 2000s, focused on lottery fraud. They used mailer to deface the website and identify consumers who could be persuaded to pay to redeem lottery tickets. A second group, called Yahooze, emerged around 2006-2007 and specialized in romance scams. They widely used the Nigerian prince scheme, in which gullible foreigners were deceived into providing money to help a supposed Nigerian prince unfreeze their assets. Many people from the Yahooze era later legitimized their wealth and now run legitimate businesses. They try to integrate into society and not draw attention to themselves. In contrast, the latest generation of Yahoos, which began around 2010, is characterized by promiscuity and recklessness. Many of them are young and inexperienced, and their wealth inflates their egos, making them loud and ostentatious.

Prevalence of Yahoo Activities during the COVID-19 Lockdown

During covid-19 and the resultant lockdown, existing records show rising incidences around the world. A study by Alawida, Omolara, Abiodun and Al-Rajaba (2022) found that since the COVID-19 crisis, there were approximately 1,872 breaches in 2020 compared to 1,108 in 2019. The pandemic prompted the medical community, as well as governments and citizens around the world to pool resources to prevent the spread of the disease. As healthcare organizations stretch their resources to combat the COVID-19 outbreak, they are unfortunately becoming the target of cyber-attacks (McKinsey & Company, 2020, TCS Worldwide, 2020; Orange Cyber Defense, 2020 cited in Alawida et al., 2022).

According to Alawida et al (2022), in addition to other cyber security concerns, fraud incidents increased by 42% compared to the previous year, with cybercriminals taking advantage of the fact that many brick-and-mortar stores have moved online. Some bank customers reported receiving text messages telling them to go online and change the delivery date of their parcels. Meanwhile, others entered their banking information, which later led to their accounts being compromised (Alawida et al, 2022). In other news,

CBS News reported on April 16, 2021 that two Indonesian hackers were caught in a $60 million fraud case. Following a tip from US authorities, two suspects were arrested in Surabaya, Indonesia's second largest city (cbsnews, 2021).

Following this increase, the US Department of Homeland Security (DHS), the UK's National Cyber Security Center (NCSC) and the Cyber Security and Infrastructure Security Agency (CISA) issued a joint advisory on April 8, 2020 describing how cybercriminals and APT organizations were exploiting the COVID-19 pandemic (Deloitte, 2020, Alawida et al, 2022). Concerns about phishing, malware and other attacks on communication networks were addressed in this advisory from organizations, such as Microsoft Teams and Zoom. As the world focuses on the health and economic challenges caused by COVID-19, cybercriminals around the world took advantage of the situation (Alawida et al., 2022). It was revealed that with the advent of COVID-19, many businesses, both large and small, fell victim to cyber-attacks, which contributed to their collapse (Lally et al., 2021). A March 2020 study reported a 5-6% increase in phishing and hacking (Naidoo, 2020). However, the number of suspicious email attacks reported provides an insight into the cybercrime challenges facing the United Kingdom and nations around the globe during the outbreak, with a significant number of phishing and theft attacks taking place (Alawida et al, 2022).

More than 160,000 suspicious email attacks were reported to the National Cyber Security Center (NCSC) in May, 2020 and by the end of the month, about £4.6 million had been lost to COVID-19-related scams, with around 11,206 victims of phishing and/or smishing campaigns (Sky News, 2020). In response, the NCSC and Her Majesty's Revenue and Customs (HMRC) shut down 471 fraudulent online shops (Tidy, 2020) and 292 fake websites (Hill, 2020). Vishing and smishing are two types of cyber fraud that criminals use to trick people into handing over money or personal information.

Also, as the number of people working remotely increased during the pandemic, ransomware attacks also increased dramatically (Chigada & Madzinga, 2021, Alawida et al., 2022). The financial sector in particular is a common target of these attacks. As many countries struggle to cope with the COVID-19 crisis, ransomware grew in both scope and intensity, harming businesses, organizations, healthcare providers and government services. According to cybersecurity experts, in October 2020, ransomware groups used DDoS attacks against victims' networks or websites as an additional tool to pressure victims into paying a ransom (Alawida et al, 2022). RagnarLocker and SunCrypt were two operations using this new method at the time. As the threat landscape changes, ransomware groups are using new attacks to exploit and use vulnerable strategies to force companies to make payment.

In addition, the number of business email compromise (BEC) attacks increased by 14% in 2020 due to the massive increase in cyber-attacks due to the COVID-19 crisis and global lockdowns. In 2020, hostile actors received 30% more rewards than the year 2019 (Alawida et al, 2022). Hackers posing as the World Health Organization (WHO) sent

messages to people's emails containing files explaining how to prevent the spread of the disease. However, according to Proofpoint, the email attachment contains no relevant information and instead infects personal computers (PCs) with malware known as AgentTesla Keylogger (Alawida et al, 2022). AgentTesla Keylogger can record all keystrokes and send them to the attackers to monitor the victim's online activities.

Upsurge in Cyber-Fraud: Understanding Victims' Susceptibility and Yahoo boys Opportunities

COVID-19 has not only changed people's general behavior, but also had a significant impact on psychological and mental health. During the pandemic, many people experienced varying degrees of emotional distress, including trauma and post-traumatic stress, depression, loneliness, generalized anxiety, insomnia, and suicidal thoughts (Lee, 2020). Additionally, individuals may avoid meeting others while paradoxically experiencing a fear of social isolation (Kumar & Nayar, 2020). Cybercriminals target these psychological vulnerabilities and exploited fears about COVID-19 by manipulating their emotional instability to launch cyber fraud. According to Naidoo (2020) research, 30% of cyber fraud incidents involve cybercriminals targeting victims and using palliatives as an emotional appeal, while 22% of cyber fraud incidents are related to fear and 22% are related to hope.

Other emotional appeals used in cyber fraud include enjoyment (15%), threat (6%) and sympathy (5%) (Naidoo, 2020). For example, to use relief or hope as emotional elements to attract targeted victim's attention, cybercriminals may spread misinformation about possible cures/treatments or government relief funds; to facilitate fear or threat, cybercriminals may circulate COVID-19- related pressures, including local outbreaks or use intimidating virus-related images to make victims feel vulnerable and concerned (Naidoo, 2020). Research shows that in the current pandemic, cybercriminals are relying on sending positive emotional appeals to their target victims for financial gain. Psychologically, it is reasonable to assume that many of the COVID-19 themed cyber fraud schemes target victims' stress, anxiety and other emotional vulnerabilities. While we believe that cybercriminals can create a variety of sophisticated fraud schemes tailored to individual circumstances, we believe it is important to understand why and how cybercriminals do what they do.

Not only did the shutdown caused by COVID-19 leave many people vulnerable to attacks, but it also lured new and existing Yahoo boys into the illicit transactions. To combat COVID-19, governments around the world instituted lockdowns in orders to reduce physical contact between residents (McKendrick, 2020). These measures led to a paradigm shift from physical to electronic platforms, expanding virtual environments and increasing interconnectivity, and increasing vulnerability to cyber-attacks (Zephyr, 2020). Criminals look for opportunities to commit crimes where people and businesses converge. This trend did not go unnoticed by yahoo boys. This is so as the rise of digitization has reduced the prospects available in the land crime sector, moving perpetrators into places where the opportunities look vast and promising.

The economic uncertainty caused by the lockdowns also led to a recent increase in online transactions and remote working which favoured fraudsters. As more and more people turn to e-commerce due to physical store closures, security controls are often ignored to quickly meet increased demand, increasing opportunities for cyber fraud (Tankowska, 2021). The sudden shift to remote work also led to an increase in fraud attacks as companies struggle to implement strong cybersecurity measures for their remote employees (Zepyr, 2020). Thus, the sudden reliance on technology significantly contributed to the increased incidence of cyber fraud during the lockdown period due to the lack of awareness and understanding of cyber security (Robertson, 2021). Despite increasing digital literacy, cyber security awareness has lagged behind, leaving many internet users vulnerable to cyber-attacks.

Theoretical Framework

In his theory of Anomie, Emile Durkheim (1893) argues that rapid social changes in organic society (in this case, the outbreak of COVID-19) lead to a state of anomie. Anomie refers to "breakdown of the ability of a society to regulate the natural drives of individuals in the face of rapid social change" (Cott, 2002, p. 96), which can lead to a state of normlessness. Anomie theory explains why some societies have higher crime rates than others (Cott, 2002). A well-organized society with a highly specialized division of labor requires adequate rules to maintain social order. Iwarimie-Jaja and Raimi (2019) aligns with this viewpoint when they argued that social order is a fallout of the presence of good governance in society. In order words, good governance generates better regulations and if regulations are inadequate, social problems such as crime are likely to arise (Cote, 2002). In a fast-paced society where people do not receive timely guidance and regulation, anomie can lead to confusion, uncertainty, fear and frustration, which can lead to the exploitation of the population by cybercriminals.

When the COVID-19 crisis began, most people were caught up in a situation of sloppy and rapid social change without clear and thorough leadership guidance. New developments such as working from home, the use of online services and providers, and the rise of online social activity all pose serious challenges to cyber security. In terms of victimization, anomie theory provides insight into why people may become victims of cyber fraud. From a criminal's perspective, Anomie theory explains why cyber fraud has become an increasingly accessible criminal activity in a rapidly changing online environment. Anomie theory offers a viable explanation for cyber fraud losses during COVID-19.

In addition, strain theory helps explain the causes of such anomalous cyber behavior in pandemic situations. Discussing the motivations and capabilities of criminals, Robert Merton (1957) developed on Durkheim's theory of Anomie, arguing that under stable social conditions, social structural tensions can still lead to criminal activity (Cott, 2002). Merton points out that each society has its own cultural and material goals worth pursuing, such as high personal worth, high wealth, high prestige, and high social status (1957). However, the appropriate institutional structures or legal channels available to

achieve such goals are not always available to everyone. Therefore, Merton developed strain theory, which states that the emphasis on achieving material gain may override the need to follow rules and leads individuals to use any means necessary, including crime, to achieve those goals under conditions of social pressure (Choi, 2015).

Through the lens of strain theory, we can see that cybercriminals may engage in criminal activities because of a perceived social need for financial gain. In particular, by applying Strain theory to the context of COVID-19, we can see how social tensions and instability, including unemployment, food shortages, and inadequate access to safe housing, can lead criminals to engage in cyber fraud. Other motivations may include self-gratification, the need for respect from peers, and even attempts to impress potential employers in organized crime environments (Wall, 2007). Strain theory sheds light on the root causes of cyber fraud during this time of significant and unique social distress.

Methods

This study adopts the qualitative research method to unravel the nexus between Covid-19 lockdown and surge in yahoo boys' activities. Data for this work came largely from secondary sources obtained from documented works available on the internet and library such as reports, articles newspapers and books. The study used the Google search engine to search for Internet resources in the area of concern focusing more on the key words "yahoo activities in Nigeria". In the selection process, priority was given to reports of cyber fraud in the COVID-19 lockdown period. The data collected were analyzed textually to achieve the objectives of the study.

Results and Discussion

At the beginning of the Covid-19 pandemic, the Nigerian government, like many other governments, imposed lockdowns to reduce the spread of the Covid-19 virus. Consequently, the lockdown forced millions of Nigerians to stay at home and rely on internet transactions, thereby increasing the use of online platforms for work and leisure (Oboh, 2020). Yahoo's activities in Nigeria grew due to this increased internet usage as more people and businesses move online. This rise in internet fraud is corroborated by a report of the Nigerian Deposit Insurance Corporation (NDIC) as shown below:

Table 1: Deposit Money Bank Fraud Cases between 2017 and 2021

Year	*2017*	*2018*	*2019*	*2020*	*2021*
Fraud Cases	26,182	37,817	52,754	146,183	211,713

Source: Augustine (2023)

The above shows that 2020 and 2021 (the period of the pandemic), recorded an unprecedented increase in the rate of yahoo crime committed against deposit money banks. Although, there is slight increase of cybercrime each year from 2017 to 2019, it skyrocketed in 2020 to more than 200%. This obviously indicate that COVID-19 and its attendant challenges contributed to the rise of yahoo activities.

Following the outbreak of the COVID-19 pandemic and the resultant lockdown, online activity in Nigeria increased by 45% (Okere, 2020). This is due to the fact that COVID-19 increased awareness of the need for technology in various parts of our economy (Okere, 2020; Raimi & Michael-Olomu, 2022). Thus, education, business and other services moved into the digital space. The crime triangle (i.e. the criminal's desire to commit a crime, the criminal's intended target and the opportunity to commit the crime), reveals that when this happen, criminals (Yahoo boys) will naturally saw it as an opportunity and thereby shifting their activities from physical to cyber space (Okere, 2020). The fact is criminals look for opportunities to commit crimes in places where people and businesses congregate, a situation which the pandemic compelled, leading to the increase as seen in the above reported cases of fraud.

Similarly, the Nigeria Inter-Bank Settlement System Plc (NIBSS) reported that, in the first nine months of 2020, fraudsters attempted 46,126 attacks and were successful in 41,979, accounting for 91% of all cases (Ayodele, 2021). NIBSS recorded a loss of over N5.2 billion from Yahoo boys' operations during this period, the highest in four years, just in a nine-month period (Ayodele, 2021). The report further revealed that while Yahoo or internet fraud is not limited to Nigeria, the total cost of fraud in Nigeria was N3.3 billion in the third quarter of 2020 compared to N499 million in the same period of 2019, due to the pandemic.

The foregoing instigated the then Inspector-General of the Nigeria Police, M.A. Adamu to alert Nigerians on the increase in the rate of fraud and cybercrime based on intelligence report (Stephens, 2020). He revealed that fraudsters had created fraudulent websites, e-commerce platforms, fake social media accounts and emails claiming to sell and provide COVID-19 medical products. NIBSS also found that Yahoo boys primarily used social engineering to manipulate people into revealing confidential information and bank details that they used to run their businesses (Ayodele, 2021). The most common is receiving text messages or emails from fraudsters posing as bank employees (Ayodele, 2021) and feigning to be selling Covid-19 related products or providing palliatives.

In addition, Yahoo boys who were previously confined to local areas expanded their scope regionally and internationally with the help of the Internet. Nigerian fraudsters took advantage of the fluidity of the internet to target the wealthy country's financial and aid systems during the pandemic. A handy example was the Senior Special Assistant to the Governor of Ogun State, Abidemi Rufai, who used the stolen identities of over 100 Washington residents to fraudulently obtain pandemic unemployment benefits from the Employment Services Department (ESD) in Washington (Olatunji, 202). According to data released by the US Federal Bureau of Investigation (FBI) in response to a Freedom of Information request, Nigerian cyber actors fraudulently obtained more than $110 million as financial recipients of fraudulent applications of aid such as benefits and loans in 2020, almost three times roughly $33.9 million reported in 2019 (Ayodele, 2021).

Another contributor to the prevalence is the economic hardship and unemployment caused by the pandemic and the resulting lockdown which led many Nigerians youth, particularly students to indulge in cybercrime. According to Mbah (2020), the elevated level of financial desperation experienced during the lockdown fuelled an increase in Yahoo activities during the lockdown. The fact is, in times of economic hardship, people turned to illegal activities, in this case Yahoo, to meet their financial needs when conventional earning methods were unavailable or insufficient due to the lockdown.

Nigeria's poverty rate is about 40%, but inflation has risen to 17% (Olaigbe, 2020). According to a World Bank Report, the pandemic pushed Nigerian families further below the poverty line, causing some to suffer from hunger (Olaigbe, 2020; Raimi, 2020). The country's unemployment rate also rose from 27.1% to 33.3% during the pandemic, a four-fold increase in five years and the second highest in the world (Olaigbe, 2020). Many Nigerians were hit hard by this unemployment and poverty crisis caused by the pandemic, turning young people specially to Yahoo and forcing a cultural reassessment of its morality. The pandemic also disrupted education and left many unengaged with few options, causing many of them turn to cyber fraud (Olaigbe 2020).

According to experts, Nigeria did not only witness an increase in the number of people attracted to Yahoo, but also in the sophistication of the tactics they use (Olaigbe, 2021). A major shift Yahoo boys' activity during this period was capitalizing on people's fear and uncertainties related to the virus. Thus, scammers came up with new scams related to COVID-19, such as offering fake test kits or selling fake personal protective equipment (PPE) (Naidoo, 2020). In addition, the widespread use of remote work and online learning increased our dependence on digital platforms and services. This change gave Yahoo Boys a larger pool of potential victims, as people in unfamiliar digital environments may be more vulnerable to fraud (Robertson, 2021).

The Anomie and Strain theories give credence to the findings of this study, i.e. the rapidly changing online environment without proper regulations and remedial structures as well as the social tensions and instability, including unemployment, food shortages, and inadequate access to safe housing, in the context of covid-19 lockdown lead many youths and criminals to engage in cyber fraud. This invariably accounts for the upsurge in cybercrime during the period.

Conclusion

The lockdown in the pandemic influenced a shift and prevalence in Yahoo activities in Nigeria, due to increased online activity, economic hardship and unemployment. Conversely, it fostered an improved emphasis on cybersecurity, to render Yahoo boys' efforts futile. As the world navigates the new normal of pandemic-induced digitization, internet security protocols and national economic development vigilance are critical to addressing this widespread problem.

Recommendations

i. It is important that law enforcement agencies remain vigilant and adapt their strategies to the evolving tactics of the Yahoo guys. Investing in advanced technologies to detect cybercrime and strengthening international cooperation can play an important role in combating their activities.
ii. In addition, education and awareness campaigns targeting vulnerable people can help prevent them from becoming victims of online fraud. By educating people about the tactics used by Yahoo Boys, the success rate of these criminals can be reduced and protect potential victims.
iii. Furthermore, financial institutions and online platforms must continue to strengthen security measures and implement robust verification processes to prevent money laundering and fraudulent transactions. Ultimately, a multi-pronged approach that includes law enforcement, technological advancement, public awareness and industry collaboration is essential to address the challenges posed by the Yahoo Boys and protect individuals and businesses from their fraudulent activities. By working together, Nigeria can reduce the impact of cybercrime on our society.

References

Adeniran, A. (2006). A Non-dependent framework for development, *This Day,* Retrieved from www.thisdayonline.com.

Alawida, M., Omolara, A. E., Abiodun, O. I. & Al-Rajaba, M., (2022). A deeper look into cybersecurity Issues in the wake of covid-19, *A Survey Journal of King Saud University - Computer and Information Sciences*, 34(10), 8176– 8206. doi: 10.1016/j.jksuci.2022.08.003

Asemota, O. J., Ogujiuba, K., Aderemi, T. A. & Mustapha, S. (2015). Modelling and forecasting teledensity using Univariate time series models: Evidence from Nigeria, *International Journal of Statistics and Applications*, 5(6), 79- 287.

Augustine, A. (2023). *Teaming up to fight fraud is not a new idea*, What's stopping Nigerian Fintechs? Tech Cabal. Retrieved from https://techcabal.com/2023/04/20/teamup-to-figh-fraud/

Ayodele, M. (2021). Five charts showing the surge in Nigeria online fraud, *Business Day.* Retrieved from https://businessday.ng/big-read/article/five-charts-showing-the-surge-in-nigeria-fraud/?

CBS News (2021). *Indonesia Arrests Hackers over $60 Million US COVID-19 Scam*, retrieved from https://www.cbsnews.com/news/us- covid-relief- hacking-hackers-arrested-indonesia-aid-program-scam/.

Centers for Disease Control and Prevention (2020). *Coronavirus disease 2019 (COVID-19),* Centers for Disease Control and Prevention", available at: www.cdc.gov/coronavirus/2019-ncov/more/scientific-brief-sars-cov-2.html

Choi, K. (2015). *Cybercriminology and digital investigation, El Paso*, Texas: LFB Scholarly Publishing.

Cimpanu, C. (2020). *FBI says cybercrime reports quadrupled during COVID-19 Pandemic*, retrieved at: https://www.zdnet.com /article/fbi-says- cybercrime-reports-quadrupled-during-covid-19-pandemic/

Cote, S. (2002). *Criminological theories: Bridging the past to the future*, Thousand Oaks, CA: Sage Publications.

Durkheim, E. (1893). *The division of labour in society, Simpson, G. (Ed.*), New York: Macmillan Ltd.

Ezea, S. (2017). Prevalence of internet fraud among Nigerian youths. *The Guardian*, Retrieved from https://guardian.ng/saturday-magazine/prevalence-of-internet-fraud-among-nigerian-youths/.

Glickman. E. (2013). The Nigerian "419" advance fee scams: Prank or peril? *Canadian Journal of African Studies*, 460-489.

Hakak, S., Khan, W. Z., Imran, M., Choo, K. K. R. & Shoaib, M. (2020). Have You been a victim of COVID-19-related cyber incidents? Survey, taxonomy and mitigation strategies, IEEE. Access, doi: 10.1109/ACCESS.2020.3006172.

Hill, M., (2020). HMRC shuts down almost 300 COVID19 Phishing scam Sites, 2020. Retrieved from https://www.infosecuritymagazine.com/news/hmrc- covid19-phishing-scams/.

Iwarimie-Jaja, D. & Raimi, L. (2018). Governance, social order and development in Nigeria. *Port Harcourt Journal of Social Sciences*, (A Publication of the Faculty of Social Sciences, University of Port Harcourt), 8(1), 295-313.

Joseph, L., & Afolabi, M. (2020). Chasing the Nigerian dream: The proliferation of cyber fraud among Nigerian youths and its effect on Nigeria's global image. *International Journal of Intellectual Discourse (IJID)*, 3(2), 409-421.

Kumar, A. & Nayar, K. R. (2020). COVID 19 and its mental health consequences, *Journal of Mental Health*, 1-2, doi: 10.1080/09638237.2020.1757052.

Kumaran, N. & Lugani, S. (2020). Identity and security: *Protecting businesses against cyber threats during COVID-19 and beyond*, Available at: https://cloud.google.com/blog/products/identitysecurity/protecting-against-cyber-threats-during-covid-19-and-beyond.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *Comp. Security*; 1-21 doi: https://doi.org/10.106/j.cose.2021.102248

Lazarus, S., & Button, M. (2023). *Online fraudsters, colonial legacies and the North-South divide in Nigeria. The conversation,* Retrieved from, https://theconversation.com/online-fraudsters-colonial-legacies-and-the-north-south-divide-in-nigeria-187879.

Lee, S. A. (2020). Coronavirus anxiety scale: A brief mental health screener for COVID-19 related, Anxiety *Death Studies*, 44(7), 393-401, doi:10.1080/07481187.2020.1748481.

Lwangu, F. (2020). *Cyber fraud increases amid COVID-19 pandemic*, Available at: https://www.bbc.co.uk/news/business-52664539

McKendrick, J. (2020). *COVID-19 and remote work: An update [Online*], Available at: https://www.forbes.com/sites/joemckendrick/2020/07/21/ covid-19- and-remote-work-an-update/?sh=7d05f3fe6788

Merton, R. K. (1957). Social structure and anomie, *American Sociological Review*, 3(5), 672-682.

Muhammad, A. (2022). *Nigerian youth and "yahoo yahoo": A disturbing trend that must be halted economic confidential*. Retrieved from, https://economicconfidential.com/2022/09/nigerian-youth-yahoo-yahoo/.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime, *European Journal of Information Systems*, 29(3) 306-321, doi: 10.1080/0960085X.2020.1771222.

NCSC, (2020). *NCSC shines light on scams being foiled via pioneering new reporting service*, Retrieved from https://www.actionfraud.police.uk/news/cyber-expertsshine-light-on-online-scams-as-british-public-flag-over160000-suspect-emails

Nigerian Centre for Disease Control NCDC (2020). Weekly epidemiological report (COVID-19). At www.ncdc.gov.ng/reports/263/2020-june-week-23/

Oboh, G. (2020). *How Nigerians are outsmarting the pandemic*, Retrieved from https://qz.com/africa/1864903/how-coronavirus-is-impacting-internet-use-in-Nigeria/

Okere, A. (2020). Surge in online transactions over COVID-19'll increase cybercrime – Olaoye halogen group CEO. *Punch*. Retrieved from https://punchng.com/surge-in-online-transaction-over-covid-19ll-increase-cybercrime-olaoye-halogen-group-ceo

Olaigbe, O. (2021). How the pandemic pulled Nigerian University students into cybercrime. *The Record*. Retrieved from https://therecord.media/how-the-pandemic-pulled-nigerian-university- students-into-cybercrime

Olatunji, H. (2021*). Abidemi Rufai, aide of Ogun governor arrested in US over '$350,000 fraud The Cable*. Retrieved from https://www.thecable.ng/abidemi-rufai-aide-of-ogun-governor-arrested- in- us-over-350k-fraud/amp

Olawoyin, O. (2021). *How much inflationary pressure do 'Yahoo boys' heap on Nigerians? Premium Times Nigeria*. Retrieved from https://www.premiumtimesng.com/business/business-data/451854-how-much-inflationary-pressure-do-yahoo-boys-heap-on-nigerians-by-oladeinde-olawoyin.html

Ogundele, A. T., Awodiran, M. A., Idem, U. J. & Anwana, E. O. (2023). Cybercrime activities and the emergence of Yahoo Boys in Nigeria, *International Conference on Cyber Management and Engineering (CyMaEn), Bangkok, Thailand*, 313-320, doi: 10.1109/CyMaEn57228.2023.10051083.

Oloworekende, A. (2019). *No more insufficient fund: Yahoo yahoo and cyber-crime's ecosystem*, Retrieved from https://republic.com.ng/ august September -2019/yahoo-yahoo-naija/.

Raimi, L. (2017). Environmental conflict, benefit captor behaviour and new class relations in the Niger Delta region. *Ofuruma: Journal of the Humanities, Special Edition on the Niger Delta*, 2017, 66-79.

Raimi, L. (2020). Assessing the COVID-19 induced stay at home measure and social defiance by the poor in Rivers State, Nigeria. *Academic Journal of Current Research, 7*(4), 97-107

Raimi, L. & Michael-Olomu, O. (2022). Imperative of digital education: A functional analysis of the impact of COVID-19 pandemic in Nigeria, *ABSU Journal of Sociology, 3*(1), 116-127.

Robertson, C. (2021). *Cybersecurity must be a priority during the transition to working from home in the COVID-19 pandemic*, Available at: https://www.bbc.co.uk/news/business-54066238

Rothan, H. A. & Byrareddy, S. N. (2020). The epidemiology and pathogenesis of coronavirus disease (COVID-19) outbreak, *Journal of Autoimmunity*, 109, doi: 10.1016/j.jaut.2020.102433.

Shi, F. (2020). *Coronavirus-related phishing*, retrieved at: https://blog.barracuda.com/2020/03/26/threatspotlight-coronavirus-related-phishing/

Sky News, (2020). *Coronavirus: Fraud victims have lost more than £4.6m to virus- related scams, 2020*, Retrieved at https://news.sky.com/story/coronavirus-fraud-victimshave-lost-more- than-4- 6m-to-virus-related-scams11996721.

Sesan, G., Soremi, B., & Oluwafemi, B. (n.d.). *Economic cost of cybercrime in Nigeria: Paradigm initiative Nigeria*, Retrieved from https://www.opennetafrica.org/?wpfb_dl=7.

Stephens, M. (2020). COVID-19 lockdown is helping yahoo boys increase their Nigeria police warns, *NaijaHomeBased*. Retrieved from https://www.naijahomebased.come/covid-19-lockdown-is-helping-yahoo-boys-increase-their-crime-nigeria-police-warns/?amp

Tankovska, H. (2021). *Impact of coronavirus (COVID-19) on online shopping in the United States as of March 2021 [Online]*, Available at: https://www.statista.com/statistics/1112595/coronavirus-impact-online-shopping-us/

Tidy, J. (2020). *Coronavirus: Israel enables emergency spy powers. BBC News,* Retrieved from https:// www.bbc.cm/news/technology-519306

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age 4,* Cambridge, UK: Polity Press.

Zephyr, E. (2020). *Cyber security in the time of COVID-19 [Online*], Available at: https://www.weforum.org/agenda/2020/04/cyber-security-threat-covid19/